

INDEPENDENCE OF THE ZEROS OF ELLIPTIC CURVE L-FUNCTIONS OVER FUNCTION FIELDS

BYUNGCHUL CHA, DANIEL FIORILLI, AND FLORENT JOUVE

ABSTRACT. The Linear Independence hypothesis (LI), which states roughly that the imaginary parts of the critical zeros of Dirichlet L -functions are linearly independent over the rationals, is known to have interesting consequences in the study of prime number races, as was pointed out by Rubinstein and Sarnak. In this paper, we prove that a function field analogue of LI holds generically within certain families of elliptic curve L -functions and their symmetric powers. More precisely, for certain algebro-geometric families of elliptic curves defined over the function field of a fixed curve over a finite field, we give strong quantitative bounds for the number of elements in the family for which the relevant L -functions have their zeros as linearly independent over the rationals as possible.

1. MOTIVATION AND THE FUNCTION FIELD SETTING

1.1. Chebychev’s bias: the classical case and the case of elliptic curves over \mathbb{Q} . The prime number theorem in arithmetic progressions asserts that prime numbers are asymptotically equally distributed among the invertible classes modulo a given integer $q \geq 1$. However Chebychev first noticed (in the case $q = 4$, see [5]) that if one only goes up to a given $x \geq 2$ the number of primes congruent to 3 modulo 4 “often exceeds” the number of those congruent to 1 modulo 4. This phenomenon called *Chebychev’s bias* has since been extensively studied and generalized. A contemporary reference containing background and presenting a systematic approach of this question is [23]. In *loc. cit.* Rubinstein and Sarnak explain precisely the role played by the Dirichlet L -function $L(s, \chi)$ for primitive characters modulo q . Notably a (wide open) conjecture referred to as LI (for Linear Independence, also called GSH, for Grand Simplicity Hypothesis, in [23]) asserts that the multiset $\{\gamma \geq 0 : L(1/2 + i\gamma, \chi) = 0\}$ where χ runs over the set of primitive Dirichlet characters modulo q , is linearly independent over \mathbb{Q} . This assumption is shown in [23] to be crucial in the study of Chebychev’s bias.

A natural analogue from arithmetic geometry one might think of is the following. Let E/\mathbb{Q} be an elliptic curve. One has the Sato–Tate conjecture (now a theorem thanks to [6], [10], and [25]) that can be seen as analogous to the prime number theorem in arithmetic progressions since it asserts that for any real numbers a, b satisfying $0 \leq a \leq b \leq \pi$, one has

$$\lim_{x \rightarrow \infty} \frac{\#\{p \leq x : E \text{ has good reduction at } p \text{ and } \theta_p \in [a, b]\}}{\pi(x)} = \frac{2}{\pi} \int_a^b \sin^2 u \, du,$$

as long as E is not a CM elliptic curve and where for a prime p of good reduction we use the Hasse bound to write $a_p(E) := p + 1 - \#E(\mathbb{F}_p) = 2\sqrt{p} \cos \theta_p$, for a unique $\theta_p \in [0, \pi]$.

Mazur [22] raises the question of the existence of a bias between the primes up to x for which $a_p(E)$ is positive and those for which it is negative. Sarnak’s framework to study this question [24] turns out to be very effective, and explains very well this race, in terms of the

zeros (and potential poles) of the symmetric powers $L(\text{Sym}^n E, s)$, conditional on a Riemann Hypothesis and a Linear Independence assumption. Sarnak also remarked that a related question can be studied by considering the sign of the summatory function of $a_p(E)/\sqrt{p}$ using the zeros of $L(E, s)$ alone. This function is

$$S(x) = -\frac{\log x}{\sqrt{x}} \sum_{p \leq x} \frac{a_p(E)}{\sqrt{p}}.$$

The associated lower and upper densities Sarnak introduces are analogous to the ones used in [23] in the classical setting:

$$\bar{\delta}(E) = \varliminf_{T \rightarrow \infty} \frac{1}{\log T} \int_2^T \mathbf{1}_{\{x: S(x) \geq 0\}}(t) \frac{dt}{t}.$$

Sarnak shows that conditionally on the Riemann Hypothesis for $L(E, s)$ and a hypothesis about the independence of the zeros of $L(E, s)$ the two limits coincide and the common value $\delta(E)$ is different from $1/2$. He also discovers a link between the value of $\delta(E)$ and the analytic rank of E . In [8] the second author pushes this analysis further and shows that (assuming the above hypotheses) large analytic rank (compared to $\sqrt{\log N_E}$, where N_E is the conductor of E) is actually equivalent to high bias (i.e. $\delta(E)$ can get arbitrarily close to 1).

From the above references it is clear that in both the residue classes mod q and the elliptic curve settings the study of Chebychev's bias and its analogues relies on highly conjectural properties of L -functions. Notably LI or the hypothesis of Bounded Multiplicity used in [8] seem highly speculative given the current state of our knowledge of the L -functions involved.

The purpose of the present paper is to give a framework where unconditional analogues of LI can be proved. This setting is geometric in nature (we focus on elliptic curves over function fields of curves over a finite field) thus much more is known about the corresponding L -functions. Consequences for analogues of the Chebychev bias in this setting are among the main subjects developed in our paper [3]. The relevance of studying the Chebychev bias in the function field setting was first pointed out by the first named author e.g. in [2].

1.2. L -functions of elliptic curves over function fields. Let q be a power of a prime number $p \neq 2, 3$. Let \mathbb{F}_q be a field of q elements and let C/\mathbb{F}_q be a smooth projective geometrically connected curve of genus g . We define $K := \mathbb{F}_q(C)$ to be the function field of C . Finally we fix an auxiliary prime $\ell \neq p$.

Let us define precisely what are the L -functions we are interested in. We follow [26, §3.1.7] to define the L -function $L(\rho, K, T)$ of any continuous, absolutely irreducible ℓ -adic representation

$$\rho: G_K \longrightarrow \text{GL}(V)$$

of the absolute Galois group G_K of K in some finite dimensional \mathbb{Q}_ℓ -vector space V . For each v , we choose a decomposition group $D_v \subset G(K)$ and we let I_v and Frob_v be the corresponding inertia group and the geometric Frobenius conjugacy class, respectively. (We will sometimes write $\text{Frob}_{\mathbb{F}, v}$ if the field of constants $\mathbb{F} \supseteq \mathbb{F}_q$ is not obvious from context.) Then, the L -function $L(\rho, K, T)$ is defined by the formal product

$$(1) \quad L(\rho, K, T) = \prod_v \det \left(1 - \rho(\text{Frob}_v) T^{\deg v} \mid V^{\rho(I_v)} \right)^{-1},$$

where $V^{\rho(I_v)}$ denotes the subspace of inertia invariants.

Given an elliptic curve E/K we focus on the continuous ℓ -adic representation

$$\rho_{\ell, E/K} : G_K \longrightarrow \text{Aut}(V_\ell(E)),$$

arising from the Galois action on $V_\ell(E) := T_\ell(E) \otimes \mathbb{Q}_\ell$, where $T_\ell(E)$ is the ℓ -adic Tate module of E/K . Because of a well known independence of ℓ property of the family $(\rho_{\ell, E/K})$ (namely $(\rho_{\ell, E/K})_\ell$ forms a compatible system of representations), the L -function $L(\rho_{\ell, E/K}, K, T)$ will often be denoted simply $L(E/K, T)$ in the sequel.

More generally for each $m \geq 1$ we may form

$$\text{Sym}^m(\rho_{\ell, E/K}) : G_K \longrightarrow \text{Aut}(\text{Sym}^m(V_\ell(E))),$$

by taking the m -th symmetric power of $\rho_{\ell, E/K}$. Again by independence of ℓ we will write $L((\text{Sym}^m E)/K, T)$ for the L -function attached to the representation $\text{Sym}^m(\rho_{\ell, E/K})$.

Let us recall the explicit form of the local factors of $L((\text{Sym}^m E)/K, T)$. The local factor of $L((\text{Sym}^m E)/K, T)$ at an unramified prime v is given by

$$(2) \quad \prod_{j=0}^m (1 - \alpha_v^{m-j} \beta_v^j T^{\deg(v)})^{-1},$$

where α_v, β_v are the (geometric) Frobenius eigenvalues at v (i.e. the numerator of the zeta function of the fiber E_v over the residue field $\mathbb{F}_{q^{\deg v}}$ is $L(E_v/\mathbb{F}_{q^{\deg v}}, T) := 1 - (\alpha_v + \beta_v)T + q^{\deg v}T^2$).

Let us recall deep classical facts following notably from work of Deligne and Grothendieck. The statement can be found (written in greater generality) in [26, §3.1.7 and §4.1]. The deepest part (iii) of the statement is a consequence of Deligne's purity result [7, §3.2.3].

Theorem 1.1. *Assuming the j -invariant of E/K is non-constant one has*

- (i) $L((\text{Sym}^m E)/K, T) \in 1 + T\mathbb{Z}[T]$.
- (ii) $L((\text{Sym}^m E)/K, T)$ satisfies the functional equation

$$(3) \quad L((\text{Sym}^m E)/K, T) = \varepsilon_m(E/K) \cdot (q^{(m+1)/2}T)^{\nu_m} \cdot L((\text{Sym}^m E)/K, 1/(q^{m+1}T))$$

where $\nu_m := \deg L((\text{Sym}^m E)/K, T)$ and $\varepsilon_m(E/K) = \pm 1$. Further one has for $m \geq 1$

$$\nu_m = \deg \mathfrak{n}_m + (m+1)(2g-2),$$

where \mathfrak{n}_m is the Artin conductor of the representation $\text{Sym}^m(\rho_{\ell, E/K})$. If $m = 1$,

$$\mathfrak{n}_1 = M + 2A,$$

where M (resp. A) denotes the locus of multiplicative (resp. additive) reduction of E/K .

- (iii) If we write

$$(4) \quad L((\text{Sym}^m E)/K, T) = \prod_{j=1}^{\nu_m} (1 - \gamma_{m,j}T),$$

for some $\gamma_{m,j}$, then each $\gamma_{m,j}$ is of absolute value $q^{(m+1)/2}$ under any complex embedding of $\overline{\mathbb{Q}_\ell}$. Moreover one has

$$\varepsilon_m(E/K)q^{\nu_m(m+1)/2} = \prod_{j=1}^{\nu_m} (-\gamma_{m,j}).$$

We deduce from Theorem 1.1 that we can define angles $\theta_{m,j} \in [0, 2\pi]$ by the equation

$$(5) \quad \gamma_{m,j} = q^{(m+1)/2} e^{i\theta_{m,j}},$$

for all $j = 1, \dots, \nu_m$ and for each $m \geq 1$.

Since our goal is to understand possible linear dependence relations among the (inverse) zeros of $L((\text{Sym}^m E)/K, T)$ we first point out that (3) might impose that $L((\text{Sym}^m E)/K, T)$ vanishes at $\pm q^{-(m+1)/2}$. First we define the *unitarized* symmetric power L -function of E/K :

$$L_u((\text{Sym}^m E)/K, T) := L((\text{Sym}^m E)/K, T/q^{(m+1)/2}),$$

which is a monic polynomial of $1 + T\mathbb{Z}[1/q^{(m+1)/2}][T]$. It is either a reciprocal or a skew reciprocal polynomial:

$$(6) \quad L_u((\text{Sym}^m E)/K, T) = \varepsilon_m(E/K) \cdot T^{\nu_m} \cdot L_u((\text{Sym}^m E)/K, 1/T).$$

This constraint is the same as the one satisfied by characteristic polynomials of isometries of symmetric inner product spaces (the determinant of the opposite of the isometry corresponding to the sign of the functional equation). This is of course no coincidence. We handle possible imposed roots (see [26, (4.1.2.1)]) by defining *reduced* symmetric power L -functions of E/K :

$$(7) \quad L_{\text{red}}((\text{Sym}^m E)/K, T) = \begin{cases} L_u((\text{Sym}^m E)/K, T)/(1 + \varepsilon_m(E/K)T), & \text{if } \nu_m \text{ is odd,} \\ L_u((\text{Sym}^m E)/K, T)/(1 - T^2), & \text{if } \nu_m \text{ is even and } \varepsilon_m(E/K) = -1, \\ L_u((\text{Sym}^m E)/K, T), & \text{otherwise.} \end{cases}$$

Note that the degree $\nu_{m,\text{red}}$ of $L_{\text{red}}((\text{Sym}^m E)/K, T)$ is necessarily even.

We want to study properties of linear independence over \mathbb{Q} of the inverse roots $\gamma_{m,j}$ given by (5), where up to reordering we assume that the first $\nu_{m,\text{red}}$ roots of $L((\text{Sym}^m E)/K, T)$ are precisely those of $L_{\text{red}}((\text{Sym}^m E)/K, T)$. These algebraic integers have modulus $q^{(m+1)/2}$ (i.e. their “reduced” versions have modulus 1) thus only the possible relations among their arguments are of interest. The relations we focus on are those of the form

$$\prod_{j=1}^{\nu_{m,\text{red}}} e^{ir_j\theta_{m,j}} = 1, \quad r_j \in \mathbb{Q},$$

or equivalently after clearing denominators,

$$\prod_{j=1}^{\nu_{m,\text{red}}} e^{in_j\theta_{m,j}} = 1, \quad n_j \in \mathbb{Z}.$$

In other words we wonder if the family $(1, \theta_{m,1}/2\pi, \dots, \theta_{m,\nu_{m,\text{red}}}/2\pi)$ is linearly independent over \mathbb{Q} . Since the main motivation of this study is to obtain meaningful results from the point of view of Chebychev’s bias for elliptic curves over function fields, we address the more general question of the existence of linear relations among the $\theta_{m,j}$ as m varies in a finite

set (as Sarnak explains the deepest results from the point of view of Chebychev's bias would follow from considering *all* symmetric power L -functions at once but unfortunately this is beyond the reach of our method). Consequently the linear relations we are truly interested in are of the form

$$\prod_{m=1}^k \left(\prod_{j=1}^{\nu_{m,\text{red}}} e^{in_{m,j}\theta_{m,j}} \right) = 1, \quad n_{m,j} \in \mathbb{Z},$$

where $k \geq 1$ is some fixed integer. Of course the functional equation (3) translates into a linear dependence relation of the type above among arguments of reciprocal roots $\gamma_{m,j}$ (precisely these relations are given by (11)). We will call those *trivial relations* and we will further denote

$$\text{Rel} \left((\gamma_{m,j})_{\substack{1 \leq j \leq \nu_{m,\text{red}} \\ 1 \leq m \leq k}} \right) = \left\{ (n_{m,j})_{\substack{1 \leq j \leq \nu_{m,\text{red}} \\ 1 \leq m \leq k}} : n_{m,j} \in \mathbb{Z} \text{ and } \prod_{m=1}^k \left(\prod_{j=1}^{\nu_{m,\text{red}}} e^{in_{m,j}\theta_{m,j}} \right) = 1 \right\}$$

for the set of multiplicative relations among inverse roots of $L_{\text{red}}(\text{Sym}^m E/K; T)$ with $1 \leq m \leq k$. We will say that this set is trivial if it consists only of trivial relations. Ordering the inverse roots as in (11) the trivial relations are concatenations of (at most) $\nu_{m,\text{red}}$ -tuples obtained by summing row vectors of the shape

$$(0, \dots, 0, 1, 0, \dots, 0, 1, 0, \dots, 0)$$

where the two nonzero coordinates are separated by $\nu_{m,\text{red}}/2 - 1$ coordinates 0.

We will study the existence of such relations among fixed families of elliptic curves over K . In Section 2 we present the specific families we focus on and state our main results (Theorem 2.3 and Theorem 2.4). Section 3 can be read mostly independently of the rest of the paper: it translates (following an idea of Girstmair) the question of independence of the zeros into a question in the representation theory of particular Weyl groups appearing as Galois groups over \mathbb{Q} of our L -functions. In Section 3 we also give the proof of a uniform version (Proposition 2.1) of a sample of one of our main results. Section 4 is the technical heart of the paper. It establishes general large sieve statements from which we deduce the proofs (in Section 5) of our main results by appealing to big monodromy statements due to Katz.

2. SOME FAMILIES OF ELLIPTIC CURVES AND GENERIC LINEAR INDEPENDENCE

Given a fixed elliptic curve E/K with non-constant j -invariant we describe two ways of constructing families of elliptic curves over K from the base curve E/K . These families are both constructed by Katz (see [14] and [15]). One of the main reasons we focus on these particular families is Katz's deep input asserting both these families have big monodromy in a sense we will make precise later.

2.1. A family of quadratic twists. We keep the notation as in the previous section. For ease of exposition we only recall standard facts about quadratic twists of E/K in the case where $C = \mathbb{P}^1$ (i.e. K is the rational function field $\mathbb{F}_q(t)$). We let $\mathcal{E} \rightarrow C$ be the corresponding minimal Weierstrass model (i.e. the identity component of the Néron model of E). This model is obtained by gluing the affine part of E/K given, say, by the Weierstrass

equation $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_q[t]$, together with a similar model “at infinity”. For each $f \in K^\times$ we consider

$$E_f: y^2 = x^3 + f^2 ax + f^3 b$$

which is a Weierstrass equation for an elliptic curve over K . The extension $K(\sqrt{f})/K$ is the smallest over which E and E_f are isomorphic (see e.g. [1, Lemma 2.4]). Thus E and E_f are isomorphic over K if and only if f is a square in K . A *quadratic twist* of E/K is an elliptic curve E_f/K such that f is not a square in K . Note that E_f is isomorphic to E_g over K if and only if there exists $c \in K^\times$ such that $f = gc^2$.

Let $\Delta \in \mathbb{F}_q(t)$ be the discriminant of E/K ; then E_f/K has discriminant $f^6 \Delta$. Therefore, away from the irreducible factors of f , the curves E and E_f have the same locus of good reduction. Let v be a place of good reduction for E and E_f . A crucial feature of quadratic twists is that for any $f \in K^\times$ one has (see e.g. [1, §2.4])

$$(8) \quad L(E_{f,v}/\mathbb{F}_{q^{\deg v}}, T) = L\left(E_v/\mathbb{F}_{q^{\deg v}}, \left(\frac{f}{v}\right) T\right),$$

where $(\frac{\cdot}{v})$ denotes the Legendre symbol of $\mathbb{F}_{q^{\deg v}}$. From the representation theoretic point of view the L -function of a quadratic twist E_f/K can be defined as the L -function of $\rho_{\ell, E/K} \otimes \chi_f$ where χ_f is the unique nontrivial K -automorphism of $K(\sqrt{f})$. This point of view makes (8) obvious.

Let us now assume that $\mathcal{E} \rightarrow C$ has at least one fiber of multiplicative reduction and fix a nonzero element $m \in \mathbb{F}_q[t]$ which vanishes at at least one point of the locus M of multiplicative reduction of $\mathcal{E} \rightarrow C$. The “twisting family” we consider was first introduced by Katz. It is the $(d+1)$ -dimensional affine variety for which the \mathbb{F} -rational points are, for any algebraic extension $\mathbb{F} \supseteq \mathbb{F}_q$,

$$(9) \quad \mathcal{F}_d(\mathbb{F}) = \{f \in \mathbb{F}[t]: f \text{ squarefree, } \deg f = d, \gcd(f, m) = 1\},$$

where $d \geq 1$ is an integer. A crucial fact in view of the study we have in mind is the following: if $f \in \mathcal{F}_d(\mathbb{F}_{q^n})$ then $\deg L(E_f/K, T)$ only depends on d and q (in particular it is independent of n so that ultimately we will let $n \rightarrow \infty$).

Fix $d \geq 2$. One may consider 1-parameter subfamilies of \mathcal{F}_d for which the kind of generic property of independence of the zeros we have in mind can be quite easily drawn from known results. A nice feature of these 1-parameter families is that they make it possible to keep track of uniformity issues with respect to the parameters. Fix $\tilde{f} \in \mathcal{F}_{d-1}(\mathbb{F}_q)$. The family we consider is the open affine curve $U_{\tilde{f}}$ with geometric points:

$$U_{\tilde{f}}(\overline{\mathbb{F}_q}) = \{c \in \overline{\mathbb{F}_q}: (c-t)\tilde{f}(t) \in \mathcal{F}_d(\overline{\mathbb{F}_q})\}.$$

If $c \in U_{\tilde{f}}(\mathbb{F}_q)$ we denote by E_c (resp. $(\gamma_{1,j}(c))_{1 \leq j \leq N_{\text{red}}}$) the quadratic twist of E by f (resp. the multiset of inverse roots of its reduced L -function, the degree of which we denote N_{red}) where $\tilde{f}(t) = (c-t)\tilde{f}(t)$.

For this subfamily of twists we can now state a sample result of “generic” linear independence of inverse roots in the case $k = 1$ (i.e. only $L(E_c/K, T)$ is considered).

Proposition 2.1. *With notation as above, there exists integers $d_0(E)$, $q_0(E)$ depending only on E such that for any $\deg L(E_c/K, T) := N \geq 5$, any $d \geq d_0(E)$, and any $q \geq q_0(E)$, the*

set of relations between zeros of the reduced L -functions L_{red} satisfies:

$$\# \left\{ c \in U_{\tilde{f}}(\mathbb{F}_q) : \text{Rel} \left((\gamma_{1,j}(c))_{1 \leq j \leq N_{\text{red}}} \right) \text{ is nontrivial} \right\} \ll N^2 q^{1-\gamma^{-1}} \log q,$$

where the implied constant depends only on the j invariant of E and, in a controlled way, on the genus g of C/\mathbb{F}_q , and where one can choose $2\gamma = 7N^2 - 7N + 4$.

We will see how this result can be deduced from the third author's result ([11, Th. 4.3] which relies in turn on a result of Hall [9]) together with general group theoretic arguments. Before presenting our two main results (one of which is a generalization of Proposition 2.1) let us give a concrete incarnation of the above statement in the case where the base elliptic curve E/K is the Legendre curve. Let $K = \mathbb{F}_q(t)$ be the rational function field over \mathbb{F}_q . We call *Legendre elliptic curve* the curve $E_{\mathcal{L}}$ given by the Weierstrass equation

$$y^2 = x(x-1)(x-t).$$

Let $\mathcal{F}_{\mathcal{L},d}$ be the corresponding twisting space (9). For any field extension \mathbb{F}/\mathbb{F}_q the set of \mathbb{F} -rational points of this affine variety is

$$\mathcal{F}_{\mathcal{L},d}(\mathbb{F}) = \{P \in \mathbb{F}[t] : P \text{ squarefree, } \deg P = d, \gcd(P, t(t-1)) = 1\}.$$

As recalled in [11, (9)] (see the references therein for a proof) we have for any quadratic twist $E_{\mathcal{L},f}$ of $E_{\mathcal{L}}$ by $f \in \mathcal{F}_{\mathcal{L},d}(\mathbb{F}_q)$:

$$N := \deg L(E_{\mathcal{L},f}/K, T) = \begin{cases} 2d & \text{if } d \text{ is even,} \\ 2d-1 & \text{if } d \text{ is odd,} \end{cases}$$

which is an integer independent of f , as expected.

Let us fix an integer $d \geq 3$ and an \mathbb{F}_p -rational element $\tilde{f} \in \mathcal{F}_{\mathcal{L},d-1}(\mathbb{F}_p)$. An immediate consequence of Proposition 2.1 combined with [11, Th. 4.7] is the following.

Corollary 2.2. *With notation as in Proposition 2.1 one has for any $d \geq 3$ and any power q of p :*

$$\#\{c \in \mathbb{F}_q : \tilde{f}(c) \neq 0, c \neq 0, 1, \text{Rel} \left((\gamma_{1,j}(c))_{1 \leq j \leq N_{\text{red}}} \right) \text{ is nontrivial} \} \ll d^2 2^{n_{\tilde{f}}} q^{1-\gamma^{-1}} \log q,$$

with an absolute implied constant, where $n_{\tilde{f}}$ is a non-negative integer depending only on \tilde{f} , and where we can choose $2\gamma = 7N^2 - 7N + 4$.

Interestingly, recent work of Ulmer [27] focuses on the quadratic twist of $E_{\mathcal{L}}$ by -1 (it is isomorphic to $E_{\mathcal{L}}$ in case -1 is a square in K) and shows that over a suitable extension \tilde{K}/K the situation regarding L -functions is in sharp contrast with what one might expect when looking at Corollary 2.2. Indeed Ulmer shows in [27, Prop. 10.1] that $L(E_{\mathcal{L},-1}/\tilde{K}, T)$ is a power of $1 - qT$ which means the phenomenon at the exact opposite of linear independence occurs for the quadratic twist $E_{\mathcal{L},-1}/\tilde{K}$.

One of our main goals is to generalize Proposition 2.1 in two different ways. First we no longer restrict to a parameter variety of dimension 1 but we consider quadratic twists by any $f \in \mathcal{F}_d(\mathbb{F}_q)$. Also we obtain a result of linear independence for the inverse zeros of an arbitrary (finite) number of *odd* symmetric power L -functions of twists E_f at once. The result is as follows.

Theorem 2.3. *Let $K = \mathbb{F}_q(C)$ be the function field of a smooth geometrically irreducible curve C/\mathbb{F}_q . Let E/K be an elliptic curve with non-constant j -invariant and whose minimal Weierstrass model $\mathcal{E} \rightarrow C$ has at least one fiber of multiplicative reduction. If $f \in \mathcal{F}_d(\mathbb{F}_{q^n})$, let ν_m be the degree (depending only on q and $\deg f = d$) of $L(\text{Sym}^m E_f/K, T)$, the m -th symmetric power L -function of the twist E_f of E over K . As before let $(\gamma_{m,j}(f))_{1 \leq j \leq \nu_m}$ be the set of inverse roots of $L(\text{Sym}^m E_f/K, T)$ (seen as a \mathbb{Q} -polynomial of degree ν_m) ordered as in (11). Let $k \geq 1$ be a fixed integer. Then for all p bigger than a constant depending only on d and k , for all big enough p -power $q := p^n$ (precisely n is bigger than a constant depending only on $\overline{\mathcal{F}_d} := \mathcal{F}_d \times \overline{\mathbb{F}_p}$) and for all d bigger than an absolute constant,*

$$\# \left\{ f \in \mathcal{F}_d(\mathbb{F}_q) : \text{Rel} \left((\gamma_{2m-1,j}(f))_{\substack{1 \leq j \leq \nu_{2m-1}, \text{red} \\ 1 \leq m \leq k}} \right) \text{ is nontrivial} \right\} \ll q^{d+1-\gamma^{-1}} \log q,$$

where one can take $2\gamma = 4 + 7 \sum_{m=1}^k \nu_{2m-1}(\nu_{2m-1} - 1)$ and where the implied constant depends only on d and k .

Let us mention that our method cannot be generalized to produce a result where even symmetric power L -functions are involved (see Lemma 5.2). Indeed looking at (8) and (2) it becomes obvious that the local factor at a place of good reduction of, say, the $2m$ -th symmetric power L -function of a quadratic twist of E coincides with the local factor of the $2m$ -th symmetric power L -function of E at the same place. In other words we would lose the crucial fact that we consider a *family* of elliptic curves and we would be left with many repetitions of a single L -function in which case LI is trivially false.

2.2. A pullback family of elliptic curves. This family is considered by Katz in [15, §7.3]. The elliptic curve we start with is a curve $E/\mathbb{F}_q(t)$ (with non-constant j -invariant) given, say, by a Weierstrass equation of the form

$$(10) \quad E: y^2 + a_1(t)y + a_3(t)xy = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t),$$

where the $a_i(t)$'s are elements of $\mathbb{F}_q(t)$. Now given any non-constant function $f \in \mathbb{F}_q(C)$ we may form the pullback curve

$$E^f: y^2 + a_1(f)y + a_3(f)xy = x^3 + a_2(f)x^2 + a_4(f)x + a_6(f),$$

obtained by substituting t by f in the equation defining E . This defines an elliptic curve $E^f/\mathbb{F}_q(C)$. The construction implies deep links between the L -functions of $E/\mathbb{F}_q(t)$ and $E^f/\mathbb{F}_q(C)$. More precisely Katz explains ([15, (7.3.9)]) that for any $n \geq 1$ one has the divisibility relation between rational polynomials:

$$L((\text{Sym}^n E)/\mathbb{F}_q(t), T) \mid L((\text{Sym}^n E^f)/\mathbb{F}_q(C), T).$$

Of course such a divisibility relation has to be taken into account when studying the potential \mathbb{Q} -linear independence of the inverse zeros of $L((\text{Sym}^n E^f)/\mathbb{F}_q(C), T)$ as f varies. Katz defines the *new part* of the symmetric power L -function of $E^f/\mathbb{F}_q(C)$:

$$L^{\text{new}}((\text{Sym}^n E^f)/\mathbb{F}_q(C), T) := \frac{L((\text{Sym}^n E^f)/\mathbb{F}_q(C), T)}{L((\text{Sym}^n E)/\mathbb{F}_q(t), T)}.$$

Relevant to our study is the existence of linear dependence relations among the inverse zeros of $L^{\text{new}}((\text{Sym}^n E^f)/\mathbb{F}_q(C), T)$, or more generally of the product over n of such L -functions with $1 \leq n \leq k$ and k fixed. To state our main result concerning the above pullback family of elliptic curves let us recall the following.

A *divisor* D on C is a formal finite \mathbb{Z} -linear combination of rational points on C . An *effective divisor* is one with non negative coefficients. The *degree* of a divisor is the sum (in \mathbb{Z}) of its coefficients. To each $f \in \mathbb{F}_q(C)$ one can associate a divisor

$$(f) := \sum_P \text{ord}_P(f) \cdot P,$$

where the sum is over rational points on C and $\text{ord}_P(f)$ denotes the natural valuation of f at P . To any divisor D on C one may attach the Riemann–Roch space

$$\mathcal{L}(D) := \{f \in K^\times : (f) + D \geq 0\} \cup \{0\}.$$

The Riemann–Roch Theorem asserts that the dimension $\ell(D)$ of $\mathcal{L}(D)$ is finite.

Theorem 2.4. *Let $K = \mathbb{F}_q(C)$ be the function field of a smooth geometrically irreducible curve C/\mathbb{F}_q of genus g . Let E/K be an elliptic curve with non-constant j -invariant and whose minimal Weierstrass model $\mathcal{E} \rightarrow C$ has at least one fiber of multiplicative reduction.*

Let D be an effective divisor on C of degree at least $2g + 3$ and let $U_{D,S}$ be the dense open subset of $\mathcal{L}(D)$ defined in §5.1. Let $n \geq 1$. If $f \in U_{D,S}(\mathbb{F}_{q^n})$ let $(\gamma_{m,j}(f)^{\text{new}})_{1 \leq j \leq \nu_m}$ be the set of inverse roots of $L^{\text{new}}((\text{Sym}^n E^f)/\mathbb{F}_{q^n}(C), T)$ (seen as a \mathbb{Q} -polynomial of degree ν_m depending only on D and q). Let $k \geq 1$ be a fixed integer. Then for all p larger than a constant depending only on $\deg D$ and k , for all big enough p -power $q := p^r$ (precisely r has to be bigger than a constant depending only on D), and for all D of degree larger than an absolute constant, one has

$$\# \left\{ f \in U_{D,S}(\mathbb{F}_q) : \text{Rel} \left((\gamma_{m,j}(f)^{\text{new}})_{\substack{1 \leq j \leq \nu_{m,\text{red}} \\ 1 \leq m \leq k}} \right) \text{ is nontrivial} \right\} \ll q^{\ell(D) - \gamma^{-1}} \log q,$$

where one can take

$$2\gamma = 4 + 7 \sum_{j=1}^k h(j), \quad h(j) := \begin{cases} \nu_j(\nu_j - 1) & \text{if } j \text{ is odd,} \\ \nu_j(\nu_j + 1) & \text{if } j \text{ is even,} \end{cases}$$

and where the implied constant depends only on D and k .

For both the quadratic twist family and the pullback family the strategy of proof of Theorem 2.3 and Theorem 2.4 relies on a representation theoretic interpretation of linear independence relations between the roots. The idea of using the Galois action on the set of relations to study them goes back to Girstmair (see references in [19]). The proofs of our results follow these ideas together with a sieving procedure as performed by Kowalski in [19] (where similar questions of independence of zeros are addressed in the context of algebro-geometric families of hyperelliptic curves over finite fields).

3. THE GALOIS THEORETIC APPROACH TO INDEPENDENCE OF THE ZEROS

Let us now describe the strategy we use to attack the general question of linear independence of zeros of \mathbb{Q} -polynomials.

3.1. The general setup. Fix an integer $k \geq 1$ and polynomials P_1, \dots, P_k with coefficients in a field E satisfying $\mathbb{Q} \subset E \subset \mathbb{C}$. For each $i \in \{1, \dots, k\}$ let K_i be the splitting field of P_i/\mathbb{Q} . We denote by M_i the set of complex roots of P_i and we view $G_i := \text{Gal}(K_i/\mathbb{Q})$ as a subgroup of permutations of M_i . Assume further that the number fields K_i are jointly linearly disjoint so that $P := P_1 \cdots P_k$ has splitting field (over \mathbb{Q}) with Galois group isomorphic to $G := G_1 \times \cdots \times G_k$. Finally let M be the (necessarily disjoint) union of the M_i 's and let $F(M)$ be the permutation representation of G associated to the action of G on the roots of P .

We are interested in the question of \mathbb{Z} -multiplicative independence of the zeros of P . Denote by $\langle M \rangle$ the multiplicative abelian group (or \mathbb{Z} -module) generated by M . Set $\langle M \rangle_{\mathbb{Q}} := \langle M \rangle \otimes_{\mathbb{Z}} \mathbb{Q}$ the \mathbb{Q} -vector space obtained by extension of scalars. The vector space $\langle M \rangle_{\mathbb{Q}}$ is equipped with a G -module structure (inherited from the Galois action on the roots). More precisely one has a G -equivariant linear map:

$$r: F(M) \rightarrow \langle M \rangle_{\mathbb{Q}},$$

with kernel the G -module of multiplicative relations $\text{Rel}_{\mathbb{Q}}(M) := \text{Rel}(M) \otimes \mathbb{Q}$. Recall that we denote, as in [19]:

$$\text{Rel}(M) = \{(n_{\alpha}) \in \mathbb{Z}^M : \prod_{\alpha \in M} \alpha^{n_{\alpha}} = 1\}.$$

Note that it makes more sense when defining $\text{Rel}(M)$ to assume the elements of M have modulus 1 (it is indeed the case in the application to L -functions we are interested in since we consider unitarized versions of these L -functions). The crucial point is that if the G -module structure of $F(M)$ is known, one can hopefully deduce the G -module structure of $\text{Rel}_{\mathbb{Q}}(M)$.

3.2. The maximal Galois group of L -functions. The elliptic curve L -functions we are interested in satisfy a functional equation of type (3). Besides the (already discussed) fact that this may impose roots, some relations (we have called *trivial relations*) are also imposed. The functional equation (3) satisfied by $L((\text{Sym}^m E)/K, T)$ implies multiplicative relations:

$$(11) \quad \gamma_{m,j} \gamma_{m,j+(\nu_{m,\text{red}}/2)} = q^{m+1}, \quad 1 \leq j \leq \nu_{m,\text{red}}/2,$$

up to reordering the roots of $L_{\text{red}}((\text{Sym}^m E)/K, T)$. Let $g := \nu_{m,\text{red}}/2$. Because of the above relations the Galois group of the splitting field of the polynomial $L_{\text{red}}((\text{Sym}^m E)/K, T)$ over \mathbb{Q} , seen as a subgroup of the symmetric group \mathfrak{S}_{2g} on the set of $2g$ symbols

$$M := \{-g, \dots, -1, 1, \dots, g\},$$

embeds in the group W_{2g} defined by either of the following equivalent conditions.

- (1) W_{2g} is the set of permutations of $2g$ letters that commute to a given involution $c \in \mathfrak{S}_{2g}$ acting without fixed points,
- (2) the group W_{2g} is the subgroup of permutations of M acting on pairs $\{i, -i\}$. This group fits the exact sequence:

$$1 \longrightarrow \{\pm 1\}^g \longrightarrow W_{2g} \longrightarrow \mathfrak{S}_g \longrightarrow 1.$$

- (3) W_{2g} is the Weyl group of the algebraic group $\text{Sp}(2g)$, i.e. the Weyl group corresponding to the root system of type C_g .

In other words an element $\sigma \in W_{2g}$ permutes the couples $(i, -i)$, $1 \leq i \leq g$ and also allows permutations within each couple. The latter permutation is called a *sign change*. A subgroup of W_{2g} of particular interest is what can be seen as its *positive part*: it acts on pairs $\{i, -i\}$ but only allowing evenly many sign changes. In other words if one defines a signature homomorphism $\text{sgn} : W_{2g} \rightarrow \{\pm 1\}$ by $\text{sgn}(\sigma) = (-1)^{\#\{\text{sign changes in } \sigma\}}$, then one has an exact sequence

$$1 \longrightarrow W_{2g}^+ \longrightarrow W_{2g} \xrightarrow{\text{sgn}} \{\pm 1\} \longrightarrow 1.$$

Conceptually the group W_{2g}^+ is the Weyl group of the root system of type D_g . See [16, end of §1] for useful comments and explanations on the expected Galois group in our context.

As explained in Section 3.1 knowledge of the representation theory of the Galois groups of the L -functions considered will be crucial. Let us therefore state a few important facts about the action of W_{2g}^+ on $M \times M$.

Lemma 3.1. *Assume $g \geq 3$. With notation as above:*

(i) *there are exactly three orbits in the action of W_{2g}^+ on $M \times M$:*

$$\Delta = \{(i, i) : i \in M\}, \quad \Delta_c = \{(i, -i) : i \in M\}, \quad O = \{(i, j) : i, j \in M, i \neq \pm j\};$$

(ii) *let $F(M)$ be the permutation representation space associated to the action of W_{2g}^+ on M . Let $(f_i)_i$ be the associated formal basis. The decomposition of $F(M)$ as a direct sum of irreducible representations of W_{2g}^+ is*

$$F(M) = \mathbf{1} \oplus G(M) \oplus H(M),$$

where

$$G(M) = \left\{ \sum_{i \in M} t_i f_i : t_i = t_{-i}, i \in M, \text{ and } \sum_{i \in M} t_i = 0 \right\},$$

$$H(M) = \left\{ \sum_{i \in M} t_i f_i : t_i = -t_{-i}, i \in M \right\}.$$

Proof. Let us start with (i). The fact that Δ is a single orbit comes from the transitivity of the action of W_{2g}^+ on M . Next pick $(i, -i)$ and $(j, -j)$ in Δ_c and assume $1 \leq i, j \leq g$. Obviously the permutation $\sigma \in W_{2g}$ satisfying $\sigma(i) = j$ (and thus $\sigma(-i) = -j$) and fixing every other element of M is an element of W_{2g}^+ since the number of sign changes of σ is 0. Now fix an element $k \in M \setminus \{i, j\}$, $1 \leq k \leq g$. This is possible since $g \geq 3$. Define $\tilde{\sigma}$ to be the permutation of W_{2g} such that $\tilde{\sigma}(i) = -j$ (and thus $\tilde{\sigma}(j) = -i$), $\tilde{\sigma}(k) = -k$, and that fixes every other element of M . Its number of sign changes is 2 therefore $\tilde{\sigma} \in W_{2g}^+$.

Now we come to O . First notice that if $(\alpha, \beta) \in O$, then $(-\alpha, \beta) \in O$ as well. To see this, pick $\gamma \in M \setminus \{\pm\alpha, \pm\beta\}$ (recall $g \geq 3$) and set $\sigma(\alpha) = -\alpha$, $\sigma(\gamma) = -\gamma$ and σ commutes with the sign change and restricts to identity outside of $\{\pm\alpha, \pm\gamma\}$. By construction $\sigma \in W_{2g}^+$ and $\sigma(\alpha, \beta) = (-\alpha, \beta)$.

Fix an element $y = (i, j) \in O$, with $1 \leq j \leq g$, as well as an element $k \in M \setminus \{\pm i\}$. Then $(i, k) \in O$. Indeed if $1 \leq k \leq g$ then the permutation $\sigma \in W_{2g}$ such that $\sigma(i) = i$, $\sigma(j) = k$ (therefore $\sigma(-j) = -k$) and that fixes every other element of M is in the kernel of sgn . Whereas if $-g \leq k \leq -1$, then define $\tilde{\sigma} \in W_{2g}$ to be the permutation satisfying $\tilde{\sigma}(j) = k$ (therefore $\tilde{\sigma}(-j) = -k$), $\tilde{\sigma}(i) = -i$, and fixing every other element of M . The

number of sign changes of $\tilde{\sigma}$ is two so $\tilde{\sigma} \in W_{2g}^+$. One has $\tilde{\sigma}(i, j) = (-i, k)$. By the above remark we deduce in turn $(i, k) \in O$. Finally if $-g \leq j \leq -1$ the same line of reasoning as above applies as well.

An easy adaptation of the above argument produces for any $k \in M \setminus \{\pm j\}$ a permutation $\sigma \in W_{2g}^+$ such that $\sigma(y) = (k, j)$. We can now prove that O is a single W_{2g}^+ -orbit: let $(i', j') \in O$. There exists $\sigma_1 \in W_{2g}^+$ such that $\sigma_1(y) = (i, j')$ (provided $j' \neq \pm i$; otherwise (i, j) can first be mapped to (j, i) and then to (i', i) or $(i', -i)$ by possibly composing with one extra permutation of W_{2g}^+) and there exists $\sigma_2 \in W_{2g}^+$ such that $\sigma_2\sigma_1(y) = \sigma_2(i, j') = (i', j')$.

Now we turn to (ii). The three spaces $\mathbf{1}$, $G(M)$ and $H(M)$ are clearly W_{2g}^+ -spaces. Let χ be the character of $F(M)$ as a W_{2g}^+ -representaion. It is enough to show that $\langle \chi, \chi \rangle = 3$ to prove (ii). Since χ is real-valued one has $\langle \chi, \chi \rangle = \langle \chi^2, \mathbf{1} \rangle$ and this last quantity is nothing but the number of W_{2g}^+ -orbits of $M \times M$ which we saw is three. \square

Let us now assume $g \geq 3$ and let \mathcal{W}_{2g} be a group satisfying

$$W_{2g}^+ \subseteq \mathcal{W}_{2g} \subseteq W_{2g}.$$

Since $[W_{2g} : W_{2g}^+] = 2$ this means that either $\mathcal{W}_{2g} = W_{2g}^+$ or $\mathcal{W}_{2g} = W_{2g}$. An important point is that even though \mathcal{W}_{2g} is not completely determined, its natural permutation representation is. Indeed Lemma 3.1 and [19, Lemma 2.1] show that the \mathcal{W}_{2g} -module $F(M)$ has the same decomposition as a direct sum of irreducible \mathcal{W}_{2g} -modules, whichever of the two groups W_{2g} , W_{2g}^+ the group \mathcal{W}_{2g} be.

As a consequence [19, Cor. 2.3] holds if one replaces W_{2g} with the k -fold cartesian product of \mathcal{W}_{2g} . Let us state the result in this case.

Corollary 3.2. *Let $k \geq 1$ and $g_i \geq 3$ be integers ($1 \leq i \leq k$). Let $\mathcal{W}^{(k)}$ be the product $\mathcal{W}_{2g_1} \times \cdots \times \mathcal{W}_{2g_k}$ of k groups of type \mathcal{W} , (this means that for each i , one has $W_{2g_i}^+ \subseteq \mathcal{W}_{2g_i} \subseteq W_{2g_i}$, where the j -th copy is seen as a permutation group of a set M_j). The group $\mathcal{W}^{(k)}$ acts naturally on the disjoint union M of the M_j 's (its j -th factor \mathcal{W}_{2g_j} acts trivially on M_i as long as $i \neq j$). Let $F(M)$ be the permutation representation corresponding to the action of $\mathcal{W}^{(k)}$ on M . It is a $(2 \sum_i g_i)$ -dimensional $\mathcal{W}^{(k)}$ -module whose decomposition as a direct sum of (geometrically) irreducible $\mathcal{W}^{(k)}$ -modules is isomorphic to*

$$\mathbf{1} \oplus \bigoplus_{1 \leq i \leq k} G(M_i) \oplus \bigoplus_{1 \leq j \leq k} H(M_j).$$

Proof. This is a direct consequence of Lemma 3.1, of [19, Lemma 2.1], and of the fact that for any finite groups G_1, G_2 , the direct sum of an irreducible G_1 -module by an irreducible G_2 -module is an irreducible $(G_1 \times G_2)$ -module. \square

Let us finally give the decomposition of $\text{Rel}_{\mathbb{Q}}(M)$ as a G -module.

Proposition 3.3. *We keep the notation as in Corollary 3.2. Let $k \geq 1$ and $g \geq 3$ be integers. Let P_1, \dots, P_k be polynomials such that for each i the Galois group of the splitting field of P_i over \mathbb{Q} is isomorphic to W_{2g_i} . Let M be the union of the roots of the polynomials P_i , $1 \leq i \leq k$. Assume that if $\alpha, \bar{\alpha}$ are elements of M such that $(\alpha, \bar{\alpha})$ is an element of the set acted on by $\mathcal{W}^{(k)}$ then $\alpha\bar{\alpha} \in \mathbb{Q}^\times$. Then one has*

$$\text{Rel}_{\mathbb{Q}}(M) = \bigoplus_{1 \leq j \leq k} \text{Rel}_{\mathbb{Q}}(M_j).$$

Moreover if $\alpha\bar{\alpha}$ is independent of α (say, it equals some constant $\mu \in \mathbb{Q}$), then for $g \geq 5$ (or $g \geq 3$ if $\mu = 1$) we have for each j :

$$\text{Rel}_{\mathbb{Q}}(M_j) = \begin{cases} \mathbf{1} \oplus G(M_j) & \text{if } \mu = 1, \\ G(M_j) & \text{otherwise.} \end{cases}$$

Proof. The argument is the same as in [19, Prop. 2.4(1)]. In particular, to exclude the possibility that $H(M_j)$ be a sub- \mathcal{W}_{2g_j} -representation of $F(M_j)$ we appeal to a group theoretic argument. If $g \geq 5$ the alternating group on five letters appears in the composition series of W_{2g}^+ and so W_{2g}^+ is not solvable. Moreover W_{2g}^+ is not abelian if $g \geq 3$. \square

3.3. The key implication and the proof of Proposition 2.1. For any given $m \geq 1$, Proposition 3.3 asserts that the trivial relations (11) form, after tensoring by \mathbb{Q} , the submodule $\mathbf{1} \oplus G(M)$ where M is the set of inverse roots of $L_{\text{red}}((\text{Sym}^m E), T)$. Hence we see that linear independence for the inverse roots will follow from the maximality of the Galois group of the splitting field of $L_{\text{red}}((\text{Sym}^m E), T)$ over \mathbb{Q} .

More generally the implication we will use to prove our main results is the following. If the Galois group of the splitting field over \mathbb{Q} of an elliptic curve L -function of the type we consider is “as big as possible” (i.e. contains W_{2g}^+ where $2g$ is the degree of the associated reduced L -function) then this L -function will exhibit no nontrivial multiplicative relations among its inverse roots. To give a first illustration of this argument let us prove Proposition 2.1.

Notation being as in Proposition 2.1 we use the following result ([11, Th. 4.3]) about maximality of the Galois group over \mathbb{Q} of the splitting field of $L_{\text{red}}(E_f/K, T)$ where E/K is a fixed elliptic curve (with non-constant j -invariant) and the polynomials f are obtained by letting c run over $U_{\tilde{f}}(\mathbb{F}_q)$. For any \mathbb{Q} -polynomial f let $\text{Gal}_{\mathbb{Q}} f$ be the Galois group of the splitting field of f over \mathbb{Q} .

Theorem 3.4 ([11]). *With notation as in §2.1 fix an elliptic curve E/K an integer $d \geq 2$ and a polynomial $\tilde{f} \in \mathcal{F}_{d-1}(\mathbb{F}_q)$. For any $c \in U_{\tilde{f}}(\overline{\mathbb{F}_q})$ let E_c/K (resp. $L_{\text{red},c}$, N_{red}) be the quadratic twist of E by $f(t) = (c-t)\tilde{f}(t)$ (resp. its reduced L -function, the common degree to all the reduced L -functions $L_{\text{red},c}$). If $N := \deg L(E_c/K, T) \geq 5$ (an integer which does not depend on c but only on d and q), $d \geq d_0(E)$, $q \geq q_0(E)$, then one has:*

$$\#\{c \in U_{\tilde{f}}(\mathbb{F}_q) : \text{Gal}_{\mathbb{Q}}(L_{\text{red},c}) \not\supset W_{N_{\text{red}}}^+\} \ll N^2 q^{1-\gamma^{-1}} \log q,$$

where the implied constant depends only on $j(E)$ and on \tilde{f} , where $d_0(E)$ and $q_0(E)$ depend only on E , and where one can choose $2\gamma = 7N^2 - 7N + 4$.

Notice that $c \in \mathbb{F}_q \setminus U_{\tilde{f}}(\mathbb{F}_q)$ if and only if c is a root of \tilde{f} or a root of m (see (9)). An immediate consequence of Theorem 3.4 is:

$$\#\{c \in \mathbb{F}_q : c \notin U_{\tilde{f}}(\mathbb{F}_q) \text{ or } \text{Gal}_{\mathbb{Q}}(L_{\text{red},c}) \not\supset W_{N_{\text{red}}}^+\} \ll N^2 q^{1-\gamma^{-1}} \log q,$$

with the same dependencies on the implied constant as in Theorem 3.4.

Proposition 2.1 then follows. Indeed any $c \in \mathbb{F}_q$ outside of the set on the left hand side of the inequality corresponds to a \mathbb{Q} -polynomial $L_{\text{red},c}$ with a \mathbb{Z} -multiplicatively independent set of zeros. To see this fix such a $c \in \mathbb{F}_q$ and apply Proposition 3.3 to $k = 1$ and $P = L_{\text{red},c}$ (formally one should rather choose $P = T^{N_{\text{red}}} L_{\text{red},c}(1/T)$ so that the roots are not confused

with their inverses, however the set of zeros of $L_{\text{red},c}$ is stable under inversion). The fact that $\text{Gal}_{\mathbb{Q}}(L_{\text{red},c}) \simeq \mathcal{W}_{N_{\text{red}}}$ concludes the proof.

Remark 3.5. We draw the reader's attention to the uniformity aspects of the inequality in Proposition 2.1. Notably we have a control on the dependency on the common degree N of the L -functions considered that we do not claim to obtain in the statement of Theorem 2.3. This comes from the fact that the proof of Proposition 2.1 relies on Theorem 3.4 that builds in turn on a Theorem of Hall ([9, Th. 6.3 and Th. 6.4]) where these uniformity issues are handled with care whereas our proof of Theorem 2.3 appeals to Strong Approximation where one loses the effectiveness required to keep track of the dependency on the degree of the L -functions.

As is certainly clear from the way we have proven Proposition 2.1 we will deduce our main results from maximality of Galois groups statements generalizing Theorem 3.4 (that will have to be adapted to the family of elliptic curves introduced in Section 2.2). This will be done via a sieving procedure (generalizing the one developed to prove [11, Th. 4.3]). A crucial input will be big ℓ -adic monodromy statements holding both for the families of Section 2.1 and Section 2.2.

4. SOME LARGE SIEVE STATEMENTS

We appeal to Kowalski's sieve for Frobenius. This technique is extensively described in [18, Chapter 8]. Refinements of it are developed and used in [11]. For the purpose of the present work an even more general sieve statement is needed. This comes first from the fact that several polynomials are to be considered at once (we are interested in the product of finitely many symmetric power L -functions of a given elliptic curve) rather than just one (as is the case in [11]).

We first give a general sieve statement without specifying the property we investigate (i.e. a statement that holds for any choice of sieving sets in the language of [18]).

Theorem 4.1. *Let \mathbb{F}_q be a finite field of q elements and characteristic p . Let V/\mathbb{F}_q be a smooth affine geometrically connected d -dimensional variety. Let $\kappa : V^{\text{cov}} \rightarrow V$ be a Galois étale cover with group \mathcal{G}_V an elementary 2-group. Assume further we are given a set of primes Λ of positive density that does not contain p such that for each $\ell \in \Lambda$, we are given a lisse sheaf $\mathcal{T}_{d,\ell}$ (of rank denoted $r(d)$) of \mathbb{F}_ℓ -vector spaces on V corresponding to a homomorphism:*

$$\rho_\ell : \pi_1(V, \bar{\eta}) \rightarrow GL(r(d), \mathbb{F}_\ell),$$

that can be pulled back to a lisse sheaf $\kappa^ \mathcal{T}_{d,\ell}$ on V^{cov} . We still denote by ρ_ℓ the corresponding representation:*

$$\rho_\ell : \pi_1(\overline{V^{\text{cov}}}, \bar{\mu}) \rightarrow GL(r(d), \mathbb{F}_\ell),$$

where $\bar{\mu}$ is a geometric generic point that κ maps to $\bar{\eta}$. Set $G_\ell := \rho_\ell(\pi_1(V, \bar{\eta}))$, $G_\ell^{\text{geom}} := \rho_\ell(\pi_1(\overline{V}, \bar{\eta}))$ and $G_\ell^{\text{geom}, \text{cov}} := \rho_\ell(\pi_1(\overline{V^{\text{cov}}}, \bar{\mu}))$ and assume

- *the product map*

$$\rho_{\ell,\ell'} : \pi_1(\overline{V^{\text{cov}}}, \bar{\mu}) \rightarrow G_{\ell,\ell'}^{\text{geom}, \text{cov}} := G_\ell^{\text{geom}, \text{cov}} \times G_{\ell'}^{\text{geom}, \text{cov}}$$

is onto for each $\ell \neq \ell' \in \Lambda$ (if $\ell = \ell'$ we define $\rho_{\ell,\ell'} := \rho_\ell$),

- *for every $\ell \in \Lambda$ one has $p \nmid \#G_\ell^{\text{geom}, \text{cov}}$.*

Let γ_0 be a representative of an element of the abelian quotient $G_\ell/G_\ell^{\text{geom}}$ (which corresponds to a union of left cosets relative to $G_\ell^{\text{geom, cov}}$) such that all the Frobenius conjugacy classes Frob_t , $t \in V(\mathbb{F}_q)$ map to γ_0 under ρ_ℓ . Then for any choice of family (indexed by Λ) of conjugacy invariant subsets Θ_ℓ of the left coset $\gamma_0 G_\ell^{\text{geom}}$ and any $L \geq 2$, one has:

(12)

$\#\{t \in V(\mathbb{F}_q) : \rho_\ell(\text{Frob}_t) \notin \Theta_\ell \text{ for all } \ell \leq L, \ell \in \Lambda\} \leq \#\mathcal{G}_V(q^d + Cq^{d-1/2}(L+1)^A)(\delta(\Lambda)H)^{-1}$
where $\delta(\Lambda)$ is the density of Λ ,

$$H = \sum_{\substack{\ell \leq L \\ \ell \in \Lambda}} \frac{\#\Theta_\ell}{\#G_\ell^{\text{geom}} - \#\Theta_\ell},$$

C is a constant depending only on \overline{V} , and $A = 7d'/2 + 1$ where d' is the dimension of a connected component of maximal dimension of the algebraic group underlying the G_ℓ 's (i.e. the algebraic group $\mathbf{G}/\mathbb{F}_\ell$ of minimal dimension such that $G_\ell \subseteq \mathbf{G}(\mathbb{F}_\ell)$).

Remark 4.2. The assumption that the Galois group \mathcal{G}_V is an elementary 2-group is not used in the proof. The reason we leave it as an assumption in the statement is because that condition holds in the context of our study of L -functions. Precisely the group \mathcal{G}_V comes from a product of maximal abelian quotients of orthogonal groups over finite fields.

Proof of Theorem 4.1. First, the sieve statement has to be refined (or restricted) so that only those t 's in $V(\mathbb{F}_q)$ such that Frob_t lies in a particular coset of $\pi_1(V, \bar{\eta})$ with respect to $\pi_1(V^{\text{cov}}, \bar{\eta})$ are considered. One needs first to fix an element $\alpha \in \mathcal{G}_V$ and sieve for the corresponding Frobenius conjugacy classes. Precisely, with notation as in the theorem set

$$X_\alpha := \{t \in V(\mathbb{F}_q) : \tilde{\kappa}(\text{Frob}_t) \in \alpha\},$$

where $\tilde{\kappa} : \pi_1(V, \bar{\eta}) \rightarrow \mathcal{G}_V$ maps Frob_t to the action of $\pi_1(V, \bar{\eta})$ on $\kappa^{-1}(t)$. Then we claim

$$\#\{t \in X_\alpha : \rho_\ell(\text{Frob}_t) \notin \tilde{\Theta}_\ell \text{ for all } \ell \leq L, \ell \in \Lambda\} \leq (q^d + Cq^{d-1/2}(L+1)^A)(\delta(\Lambda)\tilde{H})^{-1}$$

with the same notation and dependencies as in the theorem and where $\tilde{\Theta}_\ell$ is a conjugacy invariant subset of the coset of G_ℓ with respect to $G_\ell^{\text{geom, cov}}$ (the quantity \tilde{H} is defined the same way as H up to replacing Θ_ℓ (resp. G_ℓ^{geom}) by $\tilde{\Theta}_\ell$ (resp. $G_\ell^{\text{geom, cov}}$)). To prove the claim we show that we can apply the coset sieve of [18, §3.3] with adjustments as in [11]. Note that in both these papers Λ is a set containing all but finitely many primes however it is straightforward to adapt the method to a set of primes of positive density $\delta(\Lambda)$. This method is probably best described by considering the commutative diagram

$$(13) \quad \begin{array}{ccccccc} 1 & \longrightarrow & \pi_1(\overline{V^{\text{cov}}}, \bar{\mu}) & \longrightarrow & \pi_1(V, \bar{\eta}) & \xrightarrow{(\deg, \tilde{\kappa})} & \hat{\mathbb{Z}} \times \mathcal{G}_V \longrightarrow 1 \\ & & \downarrow \rho_\ell & & \downarrow \rho_\ell & & \downarrow \text{pr}_\ell \\ 1 & \longrightarrow & G_\ell^{\text{geom, cov}} & \longrightarrow & G_\ell & \longrightarrow & \Gamma_\ell \longrightarrow 1, \end{array}$$

where pr_ℓ (resp. Γ_ℓ) is the group morphism (resp. the quotient group) that makes the diagram commute.

In the terminology of [18] the coset sieve setting we use is the triple $((-1, \alpha), \Lambda, (\rho_\ell))$ where we see $(-1, \alpha)$ as a coset of $\pi_1(V, \bar{\eta})$ with respect to $\pi_1(\overline{V^{\text{cov}}}, \bar{\mu})$. The sifted set (again in the sense of [18]) attached is $(X_\alpha, \text{counting measure}, \text{Frob})$ where Frob is the map from closed

points of V to conjugacy classes of $\pi_1(V, \bar{\eta})$ mapping t to Frob_t . The claim together with the upper bound (12) then follows by applying [11, Cor. 3.7 case (1)]. Note that in *loc. cit.* we assume the algebraic group underlying the G_ℓ 's is an orthogonal group. However what we really need is merely an inequality of type

$$\#U_0(\mathbb{F}_\ell) \leq (\ell + 1)^\delta,$$

where U_0 is a connected δ -dimensional variety over \mathbb{F}_ℓ . This is a result due to Serre and we apply it to each connected component of the algebraic group underlying G_ℓ . \square

We deduce a large sieve estimate involving polynomials of the type we are investigating. In other words we show we can apply Theorem 4.1 to the concrete case where the property studied is the maximality of the Galois group within a particular family of (characteristic) polynomials. This amounts to specifying the sieving sets Θ_ℓ appearing in the statement of Theorem 4.1. Moreover we restrict to finite groups G_ℓ 's with underlying algebraic group a product of orthogonal and symplectic groups since this will be the case in the applications we have in mind.

Let us briefly recall some useful facts about orthogonal groups over finite fields of characteristic not 2. Let $O(N, \mathbb{F}_\ell)$ be the group of isometries with respect to a non-degenerate symmetric bilinear pairing Ψ on an N -dimensional \mathbb{F}_ℓ -vector space V . The derived group $\Omega(N, \mathbb{F}_\ell)$ of $O(N, \mathbb{F}_\ell)$ is the simultaneous kernel of the determinant and of the spinor norm (the group morphism from $O(N, \mathbb{F}_\ell)$ to the group of classes of \mathbb{F}_ℓ^\times modulo squares mapping a reflection r_v with respect to the orthogonal space of a non-isotropic vector v to $\Psi(v, v)$). This group has index 2 in $SO(N, \mathbb{F}_\ell)$. In the even dimensional case the order of the orthogonal group depends on the class modulo squares of the discriminant of the underlying quadratic form. Specifically (see e.g. [17, Table 2.1C]):

$$\#O(N, \mathbb{F}_\ell) = \begin{cases} 2\ell^{(\frac{N-1}{2})^2} \prod_{i=1}^{(N-1)/2} (\ell^{2i} - 1) & \text{if } N \text{ is odd,} \\ 2\ell^{\frac{N(N-2)}{4}} (\ell^{N/2} \mp 1) \prod_{i=1}^{N/2-1} (\ell^{2i} - 1) & \text{if } N \text{ is even and } \left(\frac{\text{disc } \Psi}{\ell}\right) = \pm 1, \end{cases}$$

where $(\frac{\cdot}{\ell})$ denotes the Legendre character modulo ℓ . In the even dimensional case distinct orders for orthogonal groups correspond either to a split (i.e. $(-1)^{N/2} \det \Psi$ is a square) quadratic form or to a non split \mathbb{F}_ℓ -quadratic space. One easily deduces the existence of positive constants $c_1(N), c_2(N)$ depending only on N such that

$$(14) \quad c_1(N) \leq \frac{\#O(N, \mathbb{F}_\ell)}{\ell^{\frac{N(N-1)}{2}}} \leq c_2(N),$$

independently of the parity of N and the class of the discriminant of Ψ modulo squares.

To state our next large sieve estimate we introduce some further notation and definitions. Generalizing (7) to any polynomial $f \in \mathbb{Q}[T]$ of degree N satisfying an equation of the type

$$(15) \quad T^N f(1/T) = \varepsilon(f) f(T), \quad \varepsilon(f) = \pm 1,$$

we define

$$f_{\text{red}}(T) = \begin{cases} f(T)/(1 + \varepsilon(f)T) & \text{if } N \text{ is odd,} \\ f(T)/(1 - T^2) & \text{if } N \text{ is even and } \varepsilon(f) = -1, \\ f(T) & \text{otherwise.} \end{cases}$$

Finally let $k \geq 1$ be an integer and let \mathcal{F} be a lisse \mathbb{Z}_ℓ -adic sheaf on a d -dimensional variety V/\mathbb{F}_q whose arithmetic monodromy group modulo ℓ embeds in a product of type

$$\prod_{1 \leq m \leq k} \mathbf{G}(r(d, m), \mathbb{F}_\ell),$$

where for any ring A

$$\mathbf{G}(r(d, m), A) := \begin{cases} \mathrm{O}(r(d, m), A) & \text{if } m \text{ is odd,} \\ \mathrm{CSp}(r(d, m), A) & \text{if } m \text{ is even.} \end{cases}$$

Here $r(d, m)$ denotes an integer depending only on m and d and $\mathrm{CSp}(r(d, m), A)$ is the group of symplectic similitudes of a non-degenerate $r(d, m)$ -dimensional A -module. We say that \mathcal{F} has *big geometric monodromy modulo ℓ* if there is a Galois étale cover V^{cov}/V , with group \mathcal{G}_V an elementary 2-group, whose geometric monodromy group modulo ℓ contains

$$\prod_{1 \leq m \leq k} \mathbf{G}'(r(d, m), \mathbb{F}_\ell),$$

where for any ring A

$$\mathbf{G}'(r(d, m), A) := \begin{cases} \Omega(r(d, m), A) & \text{if } m \text{ is odd,} \\ \mathrm{Sp}(r(d, m), A) & \text{if } m \text{ is even.} \end{cases}$$

Theorem 4.3. *Assumptions on V/\mathbb{F}_q are the same as in the statement of Theorem 4.1. We keep the notation as above. Let $k \geq 1$ be an integer. Let $\Lambda_{d,k}$ be a set of primes of positive density and suppose the density depends only on the dimension d of V and on k . Suppose further that for each $\ell \in \Lambda_{d,k}$ we are given a sheaf $\tilde{\mathcal{T}}_{d,k,\ell}$ of free \mathbb{Z}_ℓ -modules corresponding to a representation*

$$\tilde{\rho}_\ell : \pi_1(V, \bar{\eta}) \rightarrow \prod_{m=1}^k \mathbf{G}(r(d, m), \mathbb{Z}_\ell).$$

For $n \in \{1, \dots, k\}$ let $\tilde{\mathcal{T}}_{d,\ell}^{(n)}$ be the sheaf (with associated representation denoted $\tilde{\rho}_\ell^{(n)}$) corresponding to the composition of $\tilde{\rho}_\ell$ with projection onto the n -th factor (a sheaf with orthogonal or symplectic symmetry depending on the parity of n) and assume $(\tilde{\mathcal{T}}_{d,\ell}^{(n)})_{\ell \in \Lambda_{d,k}}$ forms a compatible system of \mathbb{Z}_ℓ -sheaves. Then $(\tilde{\mathcal{T}}_{d,k,\ell})_{\ell \in \Lambda_{d,k}}$ is a compatible system of \mathbb{Z}_ℓ -sheaves. Let $f \in V(\mathbb{F}_q)$ and

$$L_f := \det(1 - T\tilde{\rho}_\ell(\mathrm{Frob}_f)) \in \mathbb{Z}[T].$$

Assume the following conditions are fulfilled:

- (i) the system $(\tilde{\mathcal{T}}_{d,k,\ell})_{\ell \in \Lambda_{d,k}}$ has big geometric monodromy modulo ℓ for all $\ell \in \Lambda_{d,k}$, and the corresponding cover V^{cov}/V does not depend on $\ell \in \Lambda_{d,k}$,
- (ii) $p \nmid G_\ell^{g,\mathrm{cov}}$ for all $\ell \in \Lambda_{d,k}$,
- (iii) for all $\ell \in \Lambda_{d,k}$ and all m either $r(d, 2m-1)$ is odd or the orthogonal group $\mathrm{O}(r(d, 2m-1), \mathbb{F}_\ell)$ appearing corresponds to a split quadratic form over \mathbb{F}_ℓ .

Then we have for any sufficiently large power $q := p^n$ (n has to be chosen bigger than a constant depending only on \bar{V}):

$$(16) \quad \#\{f \in V(\mathbb{F}_q) : L_{f,\mathrm{red}} \text{ is reducible or } \mathrm{Gal}_{\mathbb{Q}}(L_{f,\mathrm{red}}) \text{ is not maximal}\} \ll_{d,k} q^{d-\gamma^{-1}} \log q,$$

where one can choose:

$$2\gamma = 4 + 7 \sum_{m=1}^k \tilde{h}(m), \quad \tilde{h}(m) := \begin{cases} r(d, m)(r(d, m) - 1) & \text{if } m \text{ is odd,} \\ r(d, m)(r(d, m) + 1) & \text{if } m \text{ is even.} \end{cases}$$

Here “maximal” means that the corresponding Galois group is isomorphic to $\mathcal{W}^{(k)}$ (with notation as in Corollary 3.2).

For any $1 \leq j \leq k$ let

$$L_{f,j} = \det(1 - T\tilde{\rho}_{\ell,j}(\text{Frob}_f)) \in \mathbb{Z}[T],$$

then in the above estimate $L_{f,\text{red}}$ denotes the product over even indices of $L_{f,j}$ times the product over odd indices of $L_{f,j,\text{red}}$. The implied constant in the upper bound depends only on d and k .

Proof. First note that one has trivially:

$$L_f = \prod_{1 \leq m \leq k} \det(1 - T\tilde{\rho}_\ell^{(m)}(\text{Frob}_f)),$$

so that $(\tilde{T}_{d,k,\ell})_{\ell \in \Lambda_{d,k}}$ is automatically a compatible system of \mathbb{Z}_ℓ -sheaves.

To prove (16) we follow the strategy of [19, Proof of Th. 4.3] where only sheaves exhibiting symplectic symmetry were needed. In *loc. cit.* the author recalls that in earlier work of his he defined four sets $\Theta_{i,\ell} \subseteq \text{CSp}(2g, \mathbb{F}_\ell)$, $1 \leq i \leq 4$, that detect the maximality of the Galois group of the \mathbb{Q} -polynomial investigated. Since [19, Th. 4.3] deals, as we do, with *products* of characteristic polynomials an additional sieving set (to which the index $i = 0$ is attributed) is introduced in the proof to guarantee that the Galois group obtained does not merely surject onto each factor of the product group $\mathcal{W}^{(k)}$ but is in fact equal to the whole group $\mathcal{W}^{(k)}$.

Likewise four families of sieving sets were identified in [11] (where only sheaves exhibiting orthogonal symmetry appeared) and shown to be sufficient to ensure maximality of the Galois group investigated. However we also need a suitable “zeroth” family $(\Theta_\ell^{(0)})$ (see Lemma 4.5 for the definition) of sieving sets to guarantee the maximality of the Galois group as a product group. Because of complications with orthogonal groups one needs to be extra careful in our case when handling multi-indices $\mathbf{i} = (i_1, \dots, i_k)$ where $i_m = 0$ for some odd m . This is the reason why we have to impose a particular value of the discriminant (modulo squares) of the quadratic spaces coming into play in the statement. Lemma 4.5 (the proof of which we postpone till the end of the section) asserts that we do have a lower bound on the density of sets $\Theta_\ell^{(0)}$ of type

$$\#\Theta_\ell^{(0)} / \#\Omega(r(d, m), \mathbb{F}_\ell) \gg 1,$$

for every odd m , with an implied constant depending only on $r(d, m)$.

At even indices, the family of sieving sets (Θ_ℓ) we choose is the same as in [19]. Now denoting $c_i^{(m)}$ the element (determined up to conjugation) of the Galois group of the m -th factor corresponding to the sieving set $\Theta_\ell^{(i)}$, for $1 \leq i \leq 4$, and noticing that the trivial permutation of the Galois group corresponds to the sieving sets $\Theta_\ell^{(0)}$ one deduces that in the Galois group investigated one may use sieve to detect all permutations of type

$$(1, \dots, 1, c_i^{(m)}, 1, \dots, 1),$$

for any $1 \leq i \leq 4$ and any $1 \leq m \leq k$. If all these permutations are successfully detected we conclude that the Galois group is isomorphic to $\mathcal{W}^{(k)}$. In particular, we only need to consider the $4k$ families $(\Theta_\ell^{(i)})$ (for indices \mathbf{i} as described above) for our purpose.

To be in the context of Theorem 4.1 it remains to check the linear disjointness condition for product representations $\rho_{\ell, \ell'}$, for $\ell \neq \ell' \in \Lambda_{d,k}$. Kowalski's argument ([19, Lemma 4.4]) can easily be generalized to our setting thanks to the group theoretical properties shared by the groups $\mathrm{Sp}(2n, \mathbb{F}_\ell)$ and $\Omega(n, \mathbb{F}_\ell)$: both are groups with all normal subgroups contained in the center. Let $N(q)$ be the left-hand side of (16). By the above considerations and applying Theorem 4.1 we get the inequality:

$$N(q) \leq \#\mathcal{G}_V \cdot (4k) \cdot (q^d + Cq^{d-1/2}(L+1)^A)(\delta(\Lambda_{d,k})H)^{-1},$$

for any $L \geq \min \Lambda_{d,k}$ and where one can choose

$$H = \min_{\mathbf{i}} \sum_{\ell \leq L} \left(\frac{\#\Theta_\ell^{(\mathbf{i})}}{\#\prod_{1 \leq m \leq k} \mathbf{G}'(r(d, m), \mathbb{F}_\ell)} \right),$$

and

$$A = 1 + 7 \sum_{m=1}^k \dim \mathbf{H}(r(d, m)) \quad \mathbf{H}(r(d, m)) := \begin{cases} \mathrm{O}(r(d, m)) & \text{if } m \text{ is odd,} \\ \mathrm{Sp}(r(d, m)) & \text{if } m \text{ is even.} \end{cases}$$

Then we choose L such that $CL^A = q^{1/2}$ that is $L = (qC^{-2})^{1/(2A)}$ (this quantity is greater than $\min \Lambda_{d,k}$ as long as q is a big enough power of p ; the exponent depends only on the constant C which in turn depends only on \bar{V}). Thus the choice $\gamma = 2A$ is suitable and the upper bound stated follows from the well known formulæ for the dimension of the orthogonal and symplectic groups. \square

We now state the following counterpart of Theorem 4.3 in terms of independence of the zeros.

Corollary 4.4. *Keeping notation as in Theorem 4.3 denote by $\mathcal{Z}(L_{f,\mathrm{red}})$ the (multi-) set of inverse roots of the reduced version of the polynomial L_f . Then we have*

$$\#\{f \in V(\mathbb{F}_q) : \mathrm{Rel}(\mathcal{Z}(L_{f,\mathrm{red}})) \text{ is nontrivial}\} \ll q^{d-\gamma^{-1}} \log q,$$

where one can take

$$2\gamma = 4 + 7 \sum_{m=1}^k \tilde{h}(m),$$

and where the implied constant depends only on d and k .

Proof. The argument is the same as the one used to deduce Proposition 2.1 from Theorem 3.4 (i.e. the relationship between maximality of the Galois group and independence of the zeros explained in §3.3). The functional equation satisfied by each $L_{f,m,\mathrm{red}}$ is (15) in the case where the degree is even and the sign of the functional equation is $+1$. Therefore the (multi-)set of zeros of $L_{f,\mathrm{red}}$ coincides with the (multi-)set of its inverse zeros. Proposition 3.3 states that as long as $\mathrm{Gal}_{\mathbb{Q}}(L_{f,\mathrm{red}})$ is maximal (i.e. isomorphic to a group of type $\mathcal{W}^{(k)}$) then the module of relations among the zeros of $L_{f,\mathrm{red}}$ is

$$\bigoplus_{1 \leq j \leq k} (\mathbf{1} \oplus G(M_j)),$$

i.e. it reduces to the relations imposed by the functional equation satisfied by $L_{f,\text{red}}$ (the so-called trivial relations (11)). \square

We end this section with the statement and the proof of the counting lemma needed in the proof of Theorem 4.3. For simplicity all congruences in the sequel will mean “congruences modulo the group of non-zero squares of \mathbb{F}_ℓ ”.

Lemma 4.5. *Let $N \geq 4$ be an integer and $\ell \geq 3$ be a prime number. Let f be a monic polynomial of degree N satisfying (15) then there is a non-degenerate N -dimensional quadratic \mathbb{F}_ℓ -space (V, Ψ) and an isometry γ of this space such that $\det(T - \gamma) = f(T)$. Moreover if N is even and $f(\pm 1) \neq 0$ then one has necessarily $\det \Psi \equiv f(-1)f(1)$.*

If N is even assume that the quadratic structure (V, Ψ) is split i.e. $(-1)^{N/2} \det \Psi \equiv 1$.

Let $\Omega(N, \mathbb{F}_\ell)$ be the derived group of the orthogonal group $O(V)$ and let α_ℓ be a representative of the four classes of $O(V)$ with respect to $\Omega(N, \mathbb{F}_\ell)$. If we set

$$\Theta_\ell^{(0)} := \{M \in \alpha_\ell \Omega(N, \mathbb{F}_\ell) : \det(1 - TM) \text{ is separable and split over } \mathbb{F}_\ell\}$$

then we have

$$\frac{\#\Theta_\ell^{(0)}}{\#\Omega(N, \mathbb{F}_\ell)} \gg_N 1.$$

Proof. The first part of the statement can be deduced from transfer arguments (see e.g. [13, Th. 4.1 and Prop. 6.2]).

Let us turn to the proof of the lower bound for $\#\Theta_\ell^{(0)}/\#\Omega(N, \mathbb{F}_\ell)$. We first claim that we may assume without loss of generality that $\det \alpha_\ell = 1$ and N is even (i.e. $N = N_{\text{red}}$, where we recall that the characteristic polynomial of α_ℓ satisfies (15) and where N_{red} is defined as the degree of its reduced version). Indeed we are only counting isometries that have a separable characteristic polynomial. If either N is odd or the determinant of such an isometry M is -1 the functional equation (15) will impose ± 1 (or both) to be an eigenvalue of multiplicity one of M . The corresponding eigenspace V_1 (or V_{-1} , or both) has dimension 1 and we have an orthogonal splitting (see e.g. [13, (6.3) and the references mentioned in the proof of Corollary 6.4])

$$V_{\pm 1} \perp V_{N_{\text{red}}},$$

where $V_{\pm 1}$ stands either for V_1 , V_{-1} or the orthogonal sum of both, depending on the parity of N and on the sign of $\det M$. The isometry M restricts to the non-degenerate N_{red} -dimensional quadratic space $V_{N_{\text{red}}}$ as an isometry of determinant 1. Up to imposing a split or non split quadratic structure on $V_{\pm 1}$ we can further assume $(-1)^{N/2} \det(V, \Psi) \equiv (-1)^{N_{\text{red}}/2} \det(V_{N_{\text{red}}}, \Psi)$. This proves the claim. In particular in the rest of the proof we will use the fact that the set of roots and the set of reciprocal roots of the characteristic polynomials considered are the same.

The strategy is then to apply [12, Th. 15] i.e. we reduce the question to that of counting candidate polynomials. Here these polynomials are reciprocal, monic, of degree N and split over \mathbb{F}_ℓ with pairwise distinct roots. The reduction step from the general case to the case N even and $\det = 1$ imposes the roots of the candidate polynomials to be different from ± 1 .

The structure of the candidate polynomials explains why we impose the split structure on the orthogonal group. Indeed if f is the characteristic polynomial (not vanishing at ± 1)

of an isometry of an even dimensional non-degenerate \mathbb{F}_ℓ -quadratic space (V, Ψ) one has (see [13, Prop. 6.2, Lemma 6.5])

$$\det \Psi \equiv (-1)^{N/2} \text{disc } f \equiv f(1)f(-1).$$

Here we consider polynomials f that are products of split quadratic polynomials of type $(T - \beta)(T - \beta^{-1})$. Note that

$$(1 - \beta)(1 - \beta^{-1})(-1 - \beta)(-1 - \beta^{-1}) = -(\beta - \beta^{-1})^2$$

and hence $(-1)^{N/2} \det \Psi \equiv 1$ meaning (V, Ψ) is a split quadratic \mathbb{F}_ℓ -space.

To produce the candidate polynomials we split $\mathbb{F}_\ell^\times \setminus \{\pm 1\}$ in two disjoint subsets so that inversion induces a bijection between these two subsets. There are

$$(17) \quad \binom{\frac{\ell-3}{2}}{\frac{N}{2}}$$

ways of picking $N/2$ suitable roots for the polynomials we consider (note each time we pick a root, its inverse will automatically be a root as well) all in the same one of the two subsets we have just described. Since we are only interested in isometries with prescribed spinor norm (imposed by the choice of α_ℓ) we have yet to show that a positive proportion of the polynomials constructed correspond to an isometry of prescribed spinor norm. For that purpose we use the following result due to Zassenhaus (see e.g. [13, Th. 5.1] and the references therein). For any isometry M of a quadratic (even dimensional) space V that has a characteristic polynomial f not vanishing at ± 1

$$N_{\text{Spin}}(M) \equiv f(-1).$$

Thus we want to check that the polynomials f we have constructed take values $f(-1)$ that are roughly equidistributed in $\mathbb{F}_\ell^\times / \mathbb{F}_\ell^{\times 2}$. It is enough to show that this equidistribution property holds for any quadratic factor of degree 2 of the polynomials we consider. Let $(T - \beta)(T - \beta^{-1})$ be such a factor ($\beta \in \mathbb{F}_\ell^\times \setminus \{\pm 1\}$). Its value at -1 is $2 + \beta + \beta^{-1}$ thus

$$\left(\frac{2 + \beta + \beta^{-1}}{\ell} \right) = \left(\frac{\beta^2 + 2\beta + 1}{\ell} \right) \left(\frac{\beta}{\ell} \right) = \left(\frac{\beta}{\ell} \right).$$

Thus using orthogonality relations we deduce

$$\begin{aligned} \#\{\beta \in \mathbb{F}_\ell^\times \setminus \{\pm 1\} : 2 + \beta + \beta^{-1} \text{ is a square}\} &= \frac{1}{2} \sum_{\beta \in \mathbb{F}_\ell^\times \setminus \{\pm 1\}} \left(1 + \left(\frac{2 + \beta + \beta^{-1}}{\ell} \right) \right) \\ &= \frac{\ell - 3}{2} + \frac{1}{2} \sum_{\beta \in \mathbb{F}_\ell^\times \setminus \{\pm 1\}} \left(\frac{\beta}{\ell} \right) = \frac{\ell - 3}{2} + O(1), \end{aligned}$$

with an absolute implied constant.

Using (17), the above equidistribution fact and the classical lower bound on binomial coefficients $\binom{n}{k} \geq (n/k)^k$ we deduce

$$\#\{f \in \mathbb{F}_\ell[T] : \deg f = N, f \text{ reciprocal, split, separable and } f(-1) \equiv N_{\text{Spin}}(\alpha_\ell)\} \gg_N \ell^{N/2}.$$

The lower bound stated in the lemma follows from the above lower bound combined with (14) and [12, Th. 15]. \square

Without much extra work one could keep track along the proof of the dependency on N and thus get a uniform version of the lower bound of Lemma 4.5. This was done for quite general sieving sets in [12, Lemma 16]. However for the application we have in mind in the present paper the qualitative upper bound of Lemma 4.5 suffices and for simplicity we have chosen not to include the extra details that would lead to a uniform lower bound.

5. PROOF OF THE MAIN RESULTS

In this section we prove Theorem 2.3 and Theorem 2.4. We first explain the cohomological genesis of the L -functions we study (i.e. L -functions for families of elliptic curves described in §2.1 and §2.2). As already mentioned both these families enjoy the property of having big geometric ℓ -adic monodromy. Then we explain how one deduces big monodromy modulo ℓ (for a big enough set of primes) for these families from the corresponding ℓ -adic information. Combining these ingredients all the assumptions needed for Theorem 4.3 to apply will be satisfied.

5.1. Cohomological genesis of the L -functions considered. We describe very briefly the constructions of Katz leading to the two families of elliptic curve L -functions we study.

5.1.1. The quadratic twist family. We first focus on the family of quadratic twist L -functions of §2.1.

As before let ℓ be a rational prime invertible in \mathbb{F}_q and let E/K be an elliptic curve over $K = \mathbb{F}_q(C)$ with non-constant j -invariant and minimal Weierstrass model $\mathcal{E} \rightarrow C$. There is an open dense curve with corresponding inclusion $j : U \subset C$ such that each fiber of $\varpi : \mathcal{E} \rightarrow U$ is an elliptic curve.

On U we consider the constant ℓ -adic sheaf $\overline{\mathbb{Q}}_\ell$. The sheaf $R^1\varpi_*\overline{\mathbb{Q}}_\ell$ on U built out of the constant ℓ -adic sheaf and of ϖ , is lisse of rank two, pure of weight one and everywhere tame if $p := \text{char } \mathbb{F}_q \geq 5$ (which is indeed the case throughout the paper by assumption). The Tate twist $R^1\varpi_*\overline{\mathbb{Q}}_\ell(1/2)$ of that sheaf is therefore of rank two, pure of weight zero, and symplectically self-dual (because of the Weil pairing on the elliptic curve E/K). Define the sheaf

$$\mathcal{S} := j_*R^1\varpi_*\overline{\mathbb{Q}}_\ell(1/2)$$

on \mathbb{P}^1 . The open set on which \mathcal{S} is lisse is the largest open set over which E/K has good reduction. Given $n \geq 1$ one can consider the symmetric n -th power of $R^1\varpi_*\overline{\mathbb{Q}}_\ell(1/2)$ on U (since this sheaf corresponds to a continuous ℓ -adic representation of the étale fundamental group of U (with respect to a fixed base point)). This sheaf $\text{Sym}^n R^1\varpi_*\overline{\mathbb{Q}}_\ell(1/2)$ is lisse on U of rank $n+1$, pure of weight zero, and everywhere tame. It is symplectically (resp. orthogonally) self-dual if n is odd (resp. if n is even). Using the inclusion j , one can then define

$$\mathcal{S}_n := j_*\text{Sym}^n R^1\varpi_*\overline{\mathbb{Q}}_\ell(1/2),$$

which is a geometrically irreducible middle-extension sheaf on \mathbb{P}^1 (this comes from the fact, proven in [7, §3.5.5], that $R^1\varpi_*\overline{\mathbb{Q}}_\ell(1/2)$ has SL_2 geometric monodromy).

The above sheaf-theoretic constructions can be combined with twisting operations. By a recipe described by Katz in [14, §5.2.1], there is a lisse ℓ -adic sheaf $\mathcal{T}_{d,n}$ on \mathcal{F}_d (the singular locus of \mathcal{S}_n being contained in the singular locus of \mathcal{S} for any $n \geq 1$) whose stalk at $f \in \mathcal{F}_d$ is $H^1(\mathbb{P}^1, j_*(\mathcal{S}_n \otimes \mathcal{L}_{\chi(f)}))$ (note that one might have to slightly modify what the inclusion j is so that the resulting sheaf is lisse). Here \mathcal{L}_χ denotes the Lang sheaf associated to the

Legendre character χ of \mathbb{F}_q and $\mathcal{L}_{\chi(f)} := f^* \mathcal{L}_\chi$. The key property we need is the following “big ℓ -adic monodromy” statement (see [15, Th. 7.6.7]).

Theorem 5.1 (Katz). *With notation as above, let $N_{d,n}$ denote the rank of the ℓ -adic sheaf $\mathcal{T}_{d,n}$.*

- (1) *If n is even then the lisse sheaf $\mathcal{T}_{d,n}(1/2)$ on \mathcal{F}_d is pure of weight zero and symplectically self-dual with geometric monodromy group $\mathrm{Sp}(N_{d,n})$,*
- (2) *if n is odd and E has multiplicative reduction at at least one closed point $\pi \in \mathbb{P}^1(\overline{\mathbb{F}_q})$, then the lisse sheaf $\mathcal{T}_{d,n}(1/2)$ on \mathcal{F}_d is pure of weight zero and orthogonally self-dual with geometric monodromy group $\mathrm{O}(N_{d,n})$.*

Fix an embedding $\iota : \overline{\mathbb{Q}_\ell} \hookrightarrow \mathbb{C}$; for each finite extension \mathbb{F}/\mathbb{F}_q and each $f \in \mathcal{F}_d(\mathbb{F})$, let $\Theta_{\mathbb{F},f}$ be the Frobenius conjugacy class in $\mathrm{USp}(N_{d,n})$ (resp. in $\mathrm{O}(N_{d,n}, \mathbb{R})$) corresponding to $\mathcal{T}_{d,n}(1/2)$ if $N_{d,n}$ is even (resp. odd) at $f \in \mathcal{F}_d(\mathbb{F})$. Then

$$L((\mathrm{Sym}^n \rho_{\ell,E/K}) \otimes \chi_f, T) = \det(1 - \Theta_{\mathbb{F},f} T) = \iota(\det(1 - T \mathrm{Frob}_{\mathbb{F},f} \mid \mathcal{T}_{d,n}(1/2))) ,$$

where we recall that χ_f is the unique nontrivial K -automorphism of $K(\sqrt{f})$.

Let us comment on the last sentence of the statement. The \mathbb{Q} -polynomial $L((\mathrm{Sym}^n \rho_{\ell,E/K}) \otimes \chi_f, T)$ does not coincide a priori with the symmetric power L -function of the representation giving rise to $L(E_f/K, T)$. More precisely the operations of “twisting” and “taking the n -th symmetric power” do not commute in general as the following lemma shows.

Lemma 5.2. *With notation as in Theorem 5.1 one has for every integer $n \geq 1$,*

$$L((\mathrm{Sym}^n E_f)/K, T) = \begin{cases} L((\mathrm{Sym}^n \rho_{\ell,E/K}) \otimes \chi_f, T) & \text{if } n \text{ is odd,} \\ L((\mathrm{Sym}^n E)/K, T) & \text{if } n \text{ is even.} \end{cases}$$

Proof. We want to compare the L -functions of the representations

$$\mathrm{Sym}^n (\rho_{\ell,E/K} \otimes \chi_f) \quad \text{and} \quad (\mathrm{Sym}^n \rho_{\ell,E/K}) \otimes \chi_f .$$

In each case the unramified places are the places of good reduction of E/K that do not correspond to an irreducible factor of f . Let v be a common unramified place for the two L -functions we consider. Combining (2) and the straightforward generalization of (8) to all symmetric powers $\mathrm{Sym}^n \rho_{\ell,E/K}$ we see that the local factor at v of the $2m$ -th (resp. $(2m+1)$ -th) symmetric power of the quadratic twist of E by f is exactly the same as the $2m$ -th (resp. $(2m+1)$ -th) symmetric power of the original curve E/K (resp. of the twist E_f/K).

By Chebotarev’s Density Theorem it is enough to check the local factors of both L -functions coincide at all unramified places to deduce that the L -functions are the same (or indeed that the underlying representations of the étale fundamental group of a maximal open subset on which they both are unramified are isomorphic). In the context of L -functions of elliptic curves over function fields this type of argument is used e.g. in [14, Rem. 7.0.5]. \square

Remark 5.3. (i) For our quadratic twist family of L -functions the lemma explains why we can only hope for the simultaneous independence of zeros when taking (a finite number of) odd symmetric power L -functions.

(ii) For sieving purposes it will be convenient in the case where n is even (i.e. $\mathcal{T}_{d,n}$ is symplectically self-dual), *not* to perform the “half Tate twist” as described in the statement of Theorem 5.1. The reason is that it is convenient to have an arithmetic monodromy group

that embeds in the symplectic *similitudes* $\mathrm{CSp}(2g)$ so that we can choose the multiplier of the similitudes as a sieving parameter.

5.1.2. The pullback family. Let us now turn to the interpretation of $L^{\mathrm{new}}((\mathrm{Sym}^n E^f)/\mathbb{F}_q(C), T)$ (seen as the \mathbb{Q} -polynomial defined in §2.2 starting with the elliptic curve given by (10)) as being the characteristic polynomial of the (global) geometric Frobenius morphism acting on an ℓ -adic cohomology space. The construction once again is due to Katz. Our exposition follows closely [15, §7.3] in which much more details (together with full proofs and other applications) are given.

As an auxiliary piece of data we fix an effective divisor D on C/\mathbb{F}_q satisfying $\deg D \geq 2g+3$ where we recall that g is the genus of C/\mathbb{F}_q . Let $S \subseteq \mathbf{A}^1$ be the locus of bad reduction of the curve E given by (10). Similarly to the case of the other family considered we assume S contains at least one place of multiplicative reduction and that $E/\mathbb{F}_q(t)$ has non-constant j -invariant (see [15, (7.3.2)] where Katz explicitly makes these assumptions). We let $U_{D,S}$ be the dense open subset of the Riemann–Roch space $\mathcal{L}(D)$ whose $\overline{\mathbb{F}_q}$ -valued points consists of those $f \in \mathcal{L}(D)/\overline{\mathbb{F}_q}$ whose divisor of poles is D and which are finite étale over S . In [15, §7.3.12] it is stated that for any $n \geq 1$ there is a lisse $\overline{\mathbb{Q}_\ell}$ -sheaf \mathcal{M}_n on $U_{D,S}$ (the fact that we assumed that $p \geq 5$ plays a role here) such that for any finite extension \mathbb{F}/\mathbb{F}_q and any $f \in U_{D,S}(\mathbb{F})$ one has

$$L^{\mathrm{new}}((\mathrm{Sym}^n E^f)/\mathbb{F}_q(C), T) = \det(1 - T \mathrm{Frob}_{\mathbb{F},f} | \mathcal{M}_n).$$

Moreover one has the following big monodromy statement (see [15, Th. 7.3.14, 7.3.16]) of the same type as Theorem 5.1.

Theorem 5.4 (Katz). *Let N_n be the rank of the sheaf \mathcal{M}_n .*

For any $n \geq 2$ the geometric monodromy group of \mathcal{M}_n is $\mathrm{O}(N_n)$ if n is odd and $\mathrm{Sp}(N_n)$ if n is even. In both cases for any finite extension \mathbb{F}/\mathbb{F}_q and any $f \in U_{D,S}(\mathbb{F})$ the global geometric Frobenius $\mathrm{Frob}_{\mathbb{F},f}$ acts as an isometry with respect to the associated bilinear structure.

Assuming further that $N_1 \geq 9$ the geometric monodromy group of \mathcal{M}_1 is $\mathrm{O}(N_1)$.

5.2. Big monodromy modulo ℓ . Our sieve setting imposes knowledge of the reduction modulo ℓ of the L -functions we consider modulo many primes ℓ . In this section we state a result of big monodromy modulo ℓ analogous to (and deduced from) Theorem 5.1 and Theorem 5.4. The other ingredient is the celebrated Strong Approximation Theorem [21] of Matthews, Vaserstein and Weisfeiler, enabling one to obtain big monodromy modulo ℓ for all but finitely many primes ℓ . An alternative method would consist in exploiting a Theorem of Larsen [20] that would produce a set of “good primes” of density 1.

Both these methods (Strong Approximation and Larsen’s argument) are explained in detail in [16, §7 and §9]. Here we merely quote Katz’s argument and refer the reader to *loc. cit.* for the details.

Once more the argument is simpler for sheaves exhibiting symplectic symmetry as opposed to sheaves with orthogonal symmetry. The reason is topological: the symplectic group $\mathrm{Sp}(2g)$ is a simply connected algebraic group while neither $\mathrm{O}(N)$ nor its connected component $\mathrm{SO}(N)$ are. Thus while Strong Approximation may be applied directly to a Zariski dense subgroup in the former case one has to go to the simply connected cover $\mathrm{Spin}(N)$ of $\mathrm{SO}(N)$ first in the latter case.

Let \mathcal{H}_n (resp. U) be either of the sheaves $\mathcal{T}_{d,n}$ (resp. the parameter variety \mathcal{F}_d) of Theorem 5.1 or \mathcal{M}_n (resp. the parameter variety $U_{D,S}$) of Theorem 5.4. Let \mathbf{G}/\mathbb{Z} be

either of the groups $\mathrm{Sp}(\mathrm{rk} \mathcal{H}_n)$ if n is even or $\mathrm{O}(\mathrm{rk} \mathcal{H}_n)$ if n is odd. Katz explains in [16, §9 and proof of Th. 3.1] that there exists an integer $N_0 \geq 1$ and a sheaf $\mathcal{H}_{\mathbb{Z}[1/N_0]}$ of $\mathbb{Z}[1/N_0]$ -modules such that for $\ell \nmid N_0$ the ℓ -adic geometric monodromy of \mathcal{H}_n is the ℓ -adic closure in $\mathbf{G}(\mathbb{Z}_\ell)$ of a finitely generated Zariski-dense subgroup $\Gamma_{N_0} \subseteq \mathbf{G}(\mathbb{Z}[1/N_0])$. (In *loc. cit.* Katz only considers the case where \mathcal{H}_n has orthogonal symmetry but the same argument works in the symplectic case.) We would like to apply Strong Approximation to Γ_{N_0} but again this is only directly possible in case $\mathbf{G} = \mathrm{Sp}(\mathrm{rk} \mathcal{H}_n)$. In [16, §9] Katz explains a way (for which he acknowledges R. Livné) to circumvent this difficulty by going to the spin double cover of $\mathrm{SO}(\mathrm{rk} \mathcal{H}_n)$.

Let us state the outcome of the above line of reasoning.

Proposition 5.5. *With notation as above let $\Gamma_{N_0, \mathrm{mod} \ell}$ denote the image in $\mathbf{G}(\mathbb{F}_\ell)$ of the geometric monodromy group of \mathcal{H}_n . Then this group is also the image by reduction modulo ℓ of the subgroup $\Gamma_{N_0} \subseteq \mathbf{G}(\mathbb{Z}[1/N_0])$. Moreover*

- if $\ell \nmid N_0$ and n is even then $\Gamma_{N_0, \mathrm{mod} \ell} = \mathrm{Sp}(\mathrm{rk} \mathcal{H}, \mathbb{F}_\ell)$,
- if $\ell \nmid N_0$ and n is odd then $\Gamma_{N_0, \mathrm{mod} \ell} \supset \Omega(\mathrm{rk} \mathcal{H}, \mathbb{F}_\ell)$ and the underlying quadratic form is obtained by reduction modulo ℓ of a quadratic form over $\mathbb{Z}[1/N_0]$.

The second part of the statement has to be made more explicit. To apply Theorem 4.3 we need to have a control on the discriminant of the quadratic form modulo ℓ for a positive density of primes. The above argument of Katz (from which the statement is deduced) asserts that, for n odd and as ℓ varies ($\ell \nmid N_0$), the ℓ -adic orthogonal group attached to \mathcal{H}_n forms the group of ℓ -adic points of a single “global” quadratic form. This provides us with the control we need on the discriminant of the quadratic forms modulo ℓ . If $\Delta \in \mathbb{Q}$ is the discriminant of the “global” quadratic form then Δ modulo ℓ is a square for a density $1/2$ of the primes exactly if $\Delta \in \mathbb{Z}$ is not a square (otherwise the density is 1, of course). This has to be done for several quadratic forms simultaneously. The following section provides the precise property we need.

5.3. End of the proof. We first state a few preparatory results that will help us pick the set of primes of positive density needed to apply Theorem 4.3. The first lemma requires an application of the prime number theorem.

Lemma 5.6. *For any fixed $A, B \geq 1$ and uniformly for $0 < |a| \leq (\log x)^A$ we have that*

$$\sum_{p \leq x} \left(\frac{a}{p} \right) \geq -c_A \frac{x}{(\log x)^B},$$

where c_A is a positive constant which depends on A only.

Proof. It is a well known fact that for any $b \neq 0$ with $b \not\equiv 3 \pmod{4}$, the function $\left(\frac{b}{\cdot} \right)$ is a Dirichlet character. Taking $b = 4a$, we note that

$$\sum_{p \leq x} \left(\frac{4a}{p} \right) = \sum_{p \leq x} \left(\frac{a}{p} \right) + O(1),$$

since the only prime p for which $\left(\frac{4a}{p}\right)$ is not necessarily equal to $\left(\frac{a}{p}\right)$ is $p = 2$. Since $\left(\frac{4a}{p}\right)$ is a Dirichlet character, we obtain from Siegel's Theorem that

$$\sum_{p \leq x} \left(\frac{a}{p}\right) = \varepsilon_a \text{Li}(x) + O_A \left(\frac{x}{(\log x)^A} \right),$$

where ε_a equals 1 when the character is principal, and is zero otherwise. The result follows. \square

Lemma 5.7. *Let A be a ring satisfying $\mathbb{Z} \subseteq A \subseteq \mathbb{Q}$ such that only finitely many primes are invertible in A (i.e. A is of the form $\mathbb{Z}[1/N_0]$ for some integer N_0). Let $k \geq 1$ be an integer and let $(V_j, \Psi_j)_{1 \leq j \leq k}$ be a sequence of (free of even rank r_j) non-degenerate quadratic A -modules. For each j let Δ_j be the discriminant of (V_j, Ψ_j) . For every odd prime $\ell \notin A^\times$ coprime to $\prod_j \Delta_j$ let $(V_{j,\ell}, \Psi_{j,\ell})$ be the non-degenerate quadratic \mathbb{F}_ℓ -vector space obtained by reduction modulo ℓ . The lower density of primes ℓ for which the quadratic \mathbb{F}_ℓ -vector spaces are simultaneously split is at least 2^{-k} .*

Proof. Let $\Delta'_j = (-1)^{r_j/2} \Delta_j$. The question is that of the density of primes ℓ for which the Δ'_j 's are simultaneously squares modulo ℓ . In order to give a lower bound on this density, we note that

$$\#\{\ell \leq x : \Delta'_j \equiv \square \pmod{\ell} \ \forall j\} \geq \sum_{\ell \leq x} \frac{\left(1 + \left(\frac{\Delta'_1}{\ell}\right)\right)}{2} \cdots \frac{\left(1 + \left(\frac{\Delta'_k}{\ell}\right)\right)}{2}.$$

(The difference between the left hand side and the right hand side comes from those ℓ dividing one of the Δ'_j .) Expanding the right hand side gives that for x large enough in terms of the Δ'_j 's,

$$\frac{\pi(x)}{2^k} + \frac{1}{2^k} \sum_{g=1}^k \sum_{1 \leq j_1 < \dots < j_g \leq k} \sum_{\ell \leq x} \left(\frac{\Delta'_{j_1} \cdots \Delta'_{j_g}}{\ell} \right) \geq \frac{\pi(x)}{2^k} + O_A \left(\frac{x}{(\log x)^A} \right),$$

by Lemma 5.6. The lemma follows. \square

Lemma 5.8. *Let Λ_0 be a set of primes of lower density δ_0 . Let N_1 and N_2 be positive natural numbers and let p be a fixed prime number. The set of primes*

$$\{\ell \in \Lambda_0 : (p, \ell^j + 1) = 1, 1 \leq j \leq N_1, (p, \ell^i - 1) = 1, 1 \leq i \leq N_2\}$$

has lower natural density at least

$$\delta_0 - \frac{N_1(N_1 + 1) + N_2(N_2 + 1)}{2(p - 1)}.$$

Proof. For any integer $i \geq 1$ let $\mu_i(\mathbb{F}_p)$ be the subgroup of \mathbb{F}_p^\times consisting of i -th roots of unity. Of course $\#\mu_i(\mathbb{F}_p) \leq i$ with equality if and only if $i \mid p - 1$. Let $\zeta \in \mu_i(\mathbb{F}_p)$ then the Prime Number Theorem in arithmetic progressions asserts that the set of primes congruent to ζ modulo p has density $1/(p - 1)$. Thus the density of primes ℓ that are congruent to some element of $\mu_i(\mathbb{F}_p)$ is $\#\mu_i(\mathbb{F}_p)/(p - 1)$. Summing over i we deduce that the upper density of primes ℓ lying in $\cup_{1 \leq i \leq N_2} \mu_i(\mathbb{F}_p)$ is at most $N_2(N_2 + 1)/(2(p - 1))$. We handle the condition $(p, \ell^j + 1) = 1$ (for $1 \leq j \leq N_1$) in the same way, replacing roots of unity by roots of the polynomial $X^j + 1$ that are of cardinality at most j in \mathbb{F}_p . \square

We now have all the necessary ingredients to derive Theorem 2.3 and Theorem 2.4. To begin with we invoke Theorem 5.1 and Theorem 5.4. Thanks to Proposition 5.5 and to the Goursat–Kolchin–Ribet Theorem (as stated e.g. in [4, Prop. 5.1, Lemma 5.2]) we deduce the existence of a set consisting of all prime numbers but finitely many of them such that condition (i) of Theorem 4.3 is satisfied. Let us mention here that to deduce the existence of a Galois étale cover of the parameter variety with suitable properties from Proposition 5.5, we invoke [11, Lemma 4.1].

The set of primes obtained depends only on k and on the dimension of the parameter variety (which in turn only depends on d in the case of the quadratic twist family and on the degree d of the divisor D in case of the pullback family). Using Lemma 5.7 we can shrink this set of primes so that condition (ii) of Theorem 4.3 is satisfied. This new set of primes $\Lambda_0(d, k)$ has lower density $\delta_0(d, k)$ at least 2^{-k} . We next apply Lemma 5.8 to $\Lambda_0(d, k)$. The integers N_1 and N_2 (that are the dimensions of the alternating or symmetric bilinear spaces involved) only depend on d and k so that for large enough p the quantity

$$\delta_0(d, k) - \frac{N_1(N_1 + 1) + N_2(N_2 + 1)}{2(p - 1)}$$

is positive. Thus condition (ii) of Theorem 4.3 is fulfilled for the set of primes $\Lambda_0(d, k)$. The conclusion of Theorem 4.3 follows and thus Corollary 4.4 applies to both the settings of Theorem 2.3 and Theorem 2.4 which finishes the proof of both these results.

Acknowledgements. We would like to thank E. Kowalski for several useful discussions and for pointing out to us relevant references where arguments needed in the proof of Lemma 5.2 are also used. The second author was supported by an NSERC Postdoctoral Fellowship.

REFERENCES

- [1] S. Baig and C. Hall, *Experimental data for Goldfeld’s conjecture over function fields*, Exp. Math. **21** (2012), no. 4, 362–374, DOI 10.1080/10586458.2012.671638.
- [2] B. Cha, *Chebyshev’s bias in function fields*, Compos. Math. **144** (2008), no. 6, 1351–1374.
- [3] B. Cha, D. Fiorilli, and F. Jouve, *Prime number races for elliptic curves over function fields* (2015), preprint, available at www.math.u-psud.fr/~jouve/EllCurvesBias.pdf.
- [4] N. Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151–180.
- [5] P. Chebyshev, *Lettre de M. le professeur Tchébychev à M. Fuss sur un nouveau théorème relatif aux nombres premiers contenus dans les formes $4n + 1$ et $4n + 3$* , Bull. Classe Phys. Acad. Imp. Sci. St. Petersburg **11** (1853), 208.
- [6] L. Clozel, M. Harris, and R. Taylor, *Automorphy for some l -adic lifts of automorphic mod l Galois representations*, Publ. Math. Inst. Hautes Études Sci. **108** (2008), 1–181.
- [7] P. Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252 (French).
- [8] D. Fiorilli, *Elliptic curves of unbounded rank and Chebyshev’s bias*, Int. Math. Res. Not. IMRN **18** (2014), 4997–5024.
- [9] C. Hall, *Big symplectic or orthogonal monodromy modulo l* , Duke Math. J. **141** (2008), no. 1, 179–203.
- [10] M. Harris, N. Shepherd-Barron, and R. Taylor, *A family of Calabi–Yau varieties and potential automorphy*, Ann. of Math. (2) **171** (2010), no. 2, 779–813.
- [11] F. Jouve, *Maximal Galois group of L -functions of elliptic curves*, Int. Math. Res. Not. IMRN **19** (2009), 3557–3594.
- [12] ———, *The large sieve and random walks on left cosets of arithmetic groups*, Comment. Math. Helv. **85** (2010), no. 3, 647–704.

- [13] F. Jouve and F. Rodriguez Villegas, *On the bilinear structure associated to Bezoutians*, J. Algebra **400** (2014), 161–184.
- [14] N. M. Katz, *Twisted L-functions and monodromy*, Annals of Mathematics Studies, vol. 150, Princeton University Press, Princeton, NJ, 2002.
- [15] ———, *Moments, monodromy, and perversity: a Diophantine perspective*, Annals of Mathematics Studies, vol. 159, Princeton University Press, Princeton, NJ, 2005.
- [16] ———, *Report on the irreducibility of L-functions*, Number theory, analysis and geometry, Springer, New York, 2012, pp. 321–353.
- [17] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990.
- [18] E. Kowalski, *The large sieve and its applications*, Cambridge Tracts in Mathematics, vol. 175, Cambridge University Press, Cambridge, 2008. Arithmetic geometry, random walks and discrete groups.
- [19] E. Kowalski, *The large sieve, monodromy, and zeta functions of algebraic curves. II. Independence of the zeros*, Int. Math. Res. Not. IMRN (2008).
- [20] M. Larsen, *Maximality of Galois actions for compatible systems*, Duke Math. J. **80** (1995), no. 3, 601–630.
- [21] C. R. Matthews, L. N. Vaserstein, and B. Weisfeiler, *Congruence properties of Zariski-dense subgroups. I*, Proc. London Math. Soc. (3) **48** (1984), no. 3, 514–532.
- [22] B. Mazur, *Finding meaning in error terms*, Bull. Amer. Math. Soc. (N.S.) **45** (2008), no. 2, 185–228.
- [23] M. Rubinstein and P. Sarnak, *Chebyshev’s bias*, Experiment. Math. **3** (1994), no. 3, 173–197.
- [24] P. Sarnak, *Letter to Barry Mazur on Chebyshev’s bias for $\tau(p)$* (2007), available at <http://publications.ias.edu/sarnak/>.
- [25] R. Taylor, *Automorphy for some l -adic lifts of automorphic mod l Galois representations. II*, Publ. Math. Inst. Hautes Études Sci. **108** (2008), 183–239.
- [26] D. Ulmer, *Geometric non-vanishing*, Invent. Math. **159** (2005), no. 1, 133–186.
- [27] ———, *Explicit points on the Legendre curve*, J. Number Theory **136** (2014), 165–194.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, MUHLENBERG COLLEGE, 2400 CHEW ST., ALLENTOWN, PA 18104, USA

E-mail address: cha@muhlenberg.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF OTTAWA, 585 KING EDWARD AVE, OTTAWA, ONTARIO, K1N 6N5, CANADA

E-mail address: daniel.fiorilli@uottawa.ca

DÉPARTEMENT DE MATHÉMATIQUES, BÂTIMENT 425, FACULTÉ DES SCIENCES D’ORSAY, UNIVERSITÉ PARIS-SUD 11, F-91405 ORSAY CEDEX, FRANCE

E-mail address: florent.jouve@math.u-psud.fr